Tilburg University

Duties of care and diligence against cybercrime

Tjong Tjin Tai, T.F.E.; Koops, E.J.; Op Heij, D.J.B.; E Silva, K.K.; Skorvánek, I.

Publication date:
2015

Document Version
Early version, also known as pre-print

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
Tjong Tjin Tai, T. F. E., Koops, E. J., Op Heij, D. J. B., E Silva, K. K., & Skorvánek, I. (2015). *Duties of care and diligence against cybercrime*. Tilburg University.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

March 2015

Duties of care and diligence against cybercrime

prof. T.F.E. Tjong Tjin Tai

mr. D.J.B. Op Heij

K.K. e Silva LL.M.

I. Skorvanek LL.M.

prof. B.J. Koops

Tilburg Law School, Tilburg University

Tilburg Institute for Law and Technology (TILT)

Tilburg Institute of Private law (TIP)

Content

Executive summary	7
Possibilities for improvement	9
Preface	11
1. Introduction	13
2. Scope of the research	15
2.1. Limitations of the research	15
2.2. Four jurisdictions	16
3. Duties of care and diligence as a general legal concept	17
3.1. Introduction	17
3.2. 'Zorgplicht' as a legal concept in Dutch law	17
3.2. Duties of care and diligence in other jurisdictions	19
3.3. Duties of care and diligence as an analytic framework	20
3.4. Conclusion	22
4. Causes and manifestations of cybercrime	23
4.1. Introduction	23
4.2. A case example	23
4.3. Actors involved in the prevention of cybercrime	25
4.4. Primary causes of security breaches	29
4.4.1. Introduction	29
4.4.2. Lack of user security awareness	30
4.4.3. Security of hardware and software	33
4.4.4. Conclusion	39
4.5. Two principal forms of cybercrime	40
4.5.1. Introduction	40
4.5.2. Malware	40
4.5.3. Botnets	42
4.5.4. Actions against malware and botnets	43
4.6. Two specific forms of cybercrime	45
4.6.1. Introduction	45
4.6.2. Ransomware	45
4.6.3. DDoS attacks	47
4.7. Actors and actions	49
4.8. Conclusion	51
5. Duties of care and diligence regarding three topics of cybercrime	53
5.1. Introduction	53
5.2. The Netherlands	53
5.2.1. Introduction	53
5.2.2. Private law	53
5.2.2.1. General contract and tort law	53
5.2.2.2. Software vendors	55
5.2.2.3. Internet Service Providers	59
5.2.2.4. Businesses	62
5.2.2.5. Others	62

5.2.3.	Criminal law	63
5.2.3.1.	Possible types of duties of care	63
5.2.3.2.	Duties of care for the three topics of cybercrime	66
5.2.4.	Administrative law	73
5.2.5.	Conclusion	75
5.3.	United States of America	75
5.3.1.	Introduction	75
5.3.2.	Private law	76
5.3.2.1.	General contract law	76
5.3.2.2.	General tort law	79
5.3.2.3.	Software vendors	81
5.3.2.4.	ISPs	88
5.3.2.5.	Businesses	91
5.3.3.	Criminal law	92
5.3.4.	Administrative law	94
5.3.5.	Conclusion	96
5.4.	Brazil	96
5.4.1.	Civil law	96
5.4.1.1.	Contractual torts	97
5.4.1.2.	Extra-contractual torts	100
5.4.1.3.	Preliminary conclusions regarding key actors	104
5.4.2.	Consumer Law	105
5.4.2.1.	General description of consumer law	105
5.4.2.2.	Preliminary conclusions on consumer torts	108
5.4.3.	Administrative Law	109
5.4.3.1.	Marco Civil	109
5.4.3.2.	National Telecommunications Agency Res. 632/2014	111
5.4.4.	Criminal law	112
5.4.5.	Conclusion	113
5.5.	Czech Republic	114
5.5.1.	Civil law	114
5.5.1.1.	General and special preventive duties	116
5.5.1.2.	The regimes of liability under Czech law	120
5.5.1.3.	Liability of particular types of subjects	123
5.5.1.3.1.	ISPs	123
5.5.1.3.2.	Software vendors	126
5.5.1.3.3.	Businesses	128
5.5.2.	Criminal Law	128
5.5.3.	Administrative Law	134
5.5.4.	Conclusion	135
5.6.	Conclusion	135
6.	Enforcement of duties of care and diligence	139
6.1.	Introduction	139
6.2.	The Netherlands	139
6.2.1.	Private law	139

6.2.2.	Criminal law	140
6.2.3.	Administrative law	141
6.3.	U.S.A.	142
6.3.1.	Private law	142
6.3.2.	Criminal law	143
6.3.3.	Administrative law	144
6.4.	Brazil	144
6.5.	Czech Republic	146
6.6.	Alternatives for compliance	149
6.6.1.	Introduction	149
6.6.2.	Cybersecurity insurance	149
6.6.3.	Self-regulation and soft law	150
6.6.4.	Specific intermediaries	153
6.6.5.	Arbitration	154
6.7.	Conclusion	155
7.	International norms for prevention of cybercrime	157
7.1.	Introduction	157
7.2.	Private law	157
7.3.	Criminal law	157
7.4.	ISPs, privacy rights and Internet principles	158
7.5.	Conclusion	161
8.	Improving compliance	163
8.1.	Introduction	163
8.2.	ISPs	163
8.3.	Software vendors	166
8.4.	Businesses	171
8.5.	Conclusion	173
9.	Conclusions	175
Annex 1.	Bibliography	177
Annex 2.	Legislation and case law	193
2.1.	Treaties	193
2.2.	EU legislation and case law	193
2.3.	Dutch legislation and case law	193
2.4.	U.S. legislation and case law	195
2.5.	Brazilian legislation and case law	196
2.6.	Czech legislation and case law	197
2.7.	Others	198
Annex 3.	Abbreviations	199
Annex 4.	Glossary	201
Annex 5.	Advisory committee	205
Annex 6.	External academic review	207

Executive summary

- The present report is an exploratory investigation of whether contributory parties other than criminals and private individuals may have legal duties to help combat cybercrime. The scope is limited to four jurisdictions (The Netherlands, U.S.A., Brazil, and Czech Republic) and three specific topics of cybercrime: security of hardware and software, ransomware, and DDoS attacks. The focus is on a legal analysis, preceded by a brief factual description, and closing with tentative suggestions for improvement.
- The causes and incidence of the three topics of cybercrime discussed in this research are tied up with global networks of communication, whereby purely local national government intervention may be insufficient to effectively fight cybercrime. In the relevant literature it is generally suggested that public-private partnerships would be required for combating cybercrime.
- The approach of duties of care and diligence is a regulatory mechanism in which the focus is on private action with public encouragement. It relies on fostering practices that develop their own implicit standards and culture.
- Specific parties such as Internet Service Providers (ISPs), software vendors, and businesses that are the victim of cybercrime are, in principle, well positioned to take actions against cybercrime. Albeit significant effort is taken by many companies, these efforts as a whole do not appear to have sufficient effect. The existing standards for action appear to be insufficiently specific. In addition, particular companies within these categories may do less than is possible, due to several causes.
 - ISPs in general have no legal duty to act to take preventive actions against cybercrime. They are generally exempt from liability as long as they remain passive to the content they transmit. Voluntary action by ISPs is to some extent discouraged by legal principles such as the rights to privacy and freedom of expression and the principle of net neutrality. The Netherlands has relatively detailed administrative rules regarding ISPs, compared to other jurisdictions.
 - Software vendors may have a limited duty to provide secure software, but their actual liability is insignificant as the result of limitation clauses. An exception is Brazil, which does have a form of product liability for software. Vendors have economic disincentives (a premium on being first to market with new functionality, and lack of user discrimination towards software security) against spending more effort for increasing software security. There is no administrative supervision for the software sector in general.
 - Businesses have, to some extent, a legal duty to prevent security breaches and unavailability of service through DDoS attacks. Customers have limited remedies to businesses that breach their obligations. Further action by businesses may find obstacles in a lack of security awareness or sense of urgency, limits to perceived benefits of additional security efforts, and lack of expertise.

- It should be noted that notification duties in case of security breaches have given rise to cyber insurance, whereby insurance companies check business security and may mediate in providing expert security services before and after a breach. This has a beneficial effect on security of businesses with little need for public enforcement.
- Enforcement of duties of care and diligence to prevent cybercrime has limited effect, due particularly to limitation clauses for damage, problems of proof of causality, and legal costs for instigating court procedures. Collective action appears to be the most effective instrument. Public enforcement is of limited value for these duties of care and diligence, as criminal intent is absent and administrative rules are generally rather abstract.
- There are few international norms, and these are not universally adopted. In particular, as regards secure software development there is not standard that is proven to be effective to prevent all vulnerabilities. Development of standards is hampered by a lack of information exchange.
- Insofar as it is found desirable that parties in general become more active, there are several suggestions for improvement. This would provide a level playing field by forcing less responsible companies to spend as much effort as responsible companies already do, and furthermore providing companies that desire more security with additional means to actually obtain and enforce such security. Improvement may be found by removing or clarifying legal limitations to act, providing or supporting additional incentives to act, facilitating communication on secure practices, supporting investigation of security vulnerabilities, with a focus on widely used standard software. This should be accomplished by a variety of public and private means.
- Ultimately this might lead to a conception and culture of what may be called Corporate Digital Responsibility.

Possibilities for improvement

- Given the existing obstacles to effecting duties of care and diligence to prevent or counteract cybercrime, the following several measures may be effective and feasible. These measures would presumably be more effective in combination, although such measures cannot completely prevent cybercrime. Whether to actually follow a suggestion depends on political and economic considerations which are outside the scope of this report. One should take care not to discourage companies who already do take responsibility, and rather focus on companies who are clearly negligent. Hence the stronger measures, listed after the weaker measures, should only be considered as an option last resort.
- It should be pointed out that these measures should generally be taken internationally or at least regionally (for example in the whole European Union) in order to be effective.
- With respect to *ISPs*:
 - Clarify exceptions to principles of privacy and net neutrality in a way that allows ISPs a sufficient measure of discretionary freedom to decide on actions to detect and combat cybercrime, including analysing data, filtering traffic, and limiting or closing Internet access of infected computers and other ISPs, while respecting these principles.
 - Provide ISP immunity for efforts to remove potential cybercrime-related content, coupled with additional incentives to take such efforts.
 - Encourage economic incentives for ISPs to focus on secure services, such as government procurement standards for ISP services, mandatory security audits of the businesses that hire ISPs (thereby requiring these to contract for secure services)
- With respect to *software vendors*:
 - Incentivise 'bounty programs' (with practices of responsible disclosure) for widely used mass-market software, funded by the companies where vulnerabilities were found.
 - Incentivise security services for free software (see below for businesses).
 - Effect mandatory security standards (including security by design) for all government procurement of software (and other IT services).
 - Institute mandatory disclosure obligations or notification duties regarding the security standards used in development, the security effort taken, and/or any discovery of vulnerabilities.
 - Establish supervisory agencies for enforcing security standards for widely used mass-market software, possibly with fines for gross negligence in preventing vulnerabilities.
 - Impose mandatory liability for serious security defects in widely used mass-market software, and limit exemptions for pure economic damages, or provide a right to return of insecure software. This is only a measure of last resort.

- With respect to *businesses*:
 - Develop and/or promote security best practices for businesses.
 - Support or require security audits (as a requirement for government procured goods and services, or possibly for certain sectors).
 - Take regulatory measures (such as information duties about clauses that limit liability in case of breach of contract) to strengthen the position of businesses towards negligent software vendors or IT service providers.
 - Stimulate or require publication of measures taken to ensure security, such as a security service that checks for vulnerabilities and develops patches. This applies in particular to free software (including open source software) where such service is not commonly contracted for by businesses.
 - For specific regulated sectors involving vital services: impose fixed or liquidated damages in case of unavailability of service through DDoS attacks or privacy violations through a security breach, possibly limited to cases of gross negligence only.
- Because of the limited scope of this report, these suggestions focus only on three groups of actors. It should not be overlooked that private individuals and the government should also increase their activity towards combating cybercrime, besides possible efforts taken by the actors discussed herein. The government may for example increase its efforts at prosecution of criminals, and may lead by example by voluntarily adopting the suggestions regarding businesses.

Preface

This study has been commissioned by the Dutch National Coordinator for Security and Counterterrorism, in accordance with the Dutch Cybersecurity Strategy 2 which aims at strengthening Internet security on the basis of private-public participation, with particular attention to responsibilities from relevant businesses.¹ The present research investigates these responsibilities from the perspective of duties of care and diligence (*zorgplichten*). It has been prepared in connection with the Global Conference on Cyberspace 2015, held in The Hague on 16-17 April 2015.

The research has been performed by prof. T.F.E. Tjong Tjin Tai in collaboration with mr. D.J.B. Op Heij (U.S. law, together with T.F.E. Tjong Tjin Tai), K.K. e Silva LL.M. (Brazilian law), I. Skorvanek LL.M. (Czech law), and prof. B.J. Kooops (Dutch criminal law and general support). General supervision and support was provided by prof. J.E.J. Prins, who has already for several years pointed out the relevance of duties of care and diligence of contributory actors for the prevention of cybercrime.²

We would like to acknowledge the contribution of the academic reviewers (see annex 6) in reviewing the U.S., Czech and Brazilian parts of the report. Furthermore we are grateful for additional information provided by Mr. Kyle D. Bryant (Regional Cyber Manager for Continental Europe at ACE Group), research assistance by Marit Vink and Thomas van Alphen, and editorial work by Claudia Quelle.

Tilburg, February 2015.

1 Nationale Cybersecurity Strategie 2, see NCSS 2013.

2 Prins 2007 and 2013.

1. Introduction

Cybercrime has become a worldwide problem. As computers are everywhere, from large Internet servers to tiny smart watches, the opportunities for abuse are enormous. The increasing dependence of society on the availability of secure computing power makes it imperative that the threat of cybercrime can be contained. Considerable effort has been and is being expended to combat viruses, computer hacking and fraud. Simultaneously, new forms of cybercrime appear: DDoS-attacks, ransomware, identity theft. It seems extraordinarily difficult to keep up with the ingenuity of criminals.

The focus of prevention of cybercrime is usually on the criminals and on the victims, as these are the parties that are directly concerned with the cybercrime and thereby in the best position to take action to avoid the crime. However, it is often remarked that other parties may also be in the position to take action. The question is: are they obliged to do so? And are there legislative or other regulatory proposals that might improve matters? That is what this report aims to answer.

This is in line with modern insights in regulation and governance which recognise that combating undesirable behaviour may depend on a combination of diverse forms of regulation and enforcement, whereby public and private law would work in tandem.³ While this diminishes the coordinating role of the traditional law enforcement, it is expected to increase effectiveness. However, an analysis from such a variety of perspectives is difficult to complete, in particular as each perspective may have its own vocabulary and approach.

In this report, we use the unifying conceptual tool of ‘duties of care and diligence’. This concept, originating from Dutch law, provides a unifying framework for describing the variety of preventive obligations that may rest on the parties involved in the occurrence and possible prevention of cybercrime.⁴ With the aid of this concept we will investigate three topics of cybercrime: ransomware, DDoS-attacks, and security of software and hardware. We will first analyse these aspects on their own to determine the opportunities for prevention, as such opportunities are a necessary precondition of the occurrence of a ‘duty of care and diligence’.

The structure of this report is as follows. Chapter 2 draws the boundaries of the research, and defines the roles of the central actors discussed in this report. Chapter 3 is a conceptual description and justification of the use of the concept of ‘duties of care and diligence’. Chapter 4 provides a factual and technical overview of the problem of cybercrime, with particular attention to the three topics under consideration here. It will culmi-

3 This is generally recognised as regards combating cybercrime, see OECD 2012a: 13, 15, 31 and 32, cons. 23 of Directive 2013/40/EU, the European Union Cybersecurity strategy JOIN(2013) 1 final, White House Summit on Cybersecurity and Consumer Protection, <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit>, also Brenner 2004b.

4 See already about the applicability of such duties to cybercrime: Prins 2007 and 2013.

nate in a list of relevant actors and the possible actions against cybercrime that they might take. Again the question is: are they obliged to take such actions?

Chapter 5 will investigate this question. An analysis of the law in four jurisdictions will provide a provisional answer as to which legal obligations rest on the most important actors that could contribute to the prevention of cybercrime. Following this, chapter 6 examines whether any existing obligations are actually enforced. In chapter 7 we will discuss international norms relevant to the prevention of cybercrime.

The outcome of chapters 5 and 7 is that existing legal duties of care and diligence for preventing cybercrime are limited and that enforcement may prove difficult. Simply imposing higher standards in a specific statute is not a sufficient solution, given the inadequacy of current standards. To supplement this analysis, Chapter 8 discusses some alternate strategies to improve compliance with more extensive duties of care and diligence. These provide inspiration for some provisional suggestions that might improve compliance.

Chapter 9 sums up the conclusions drawn from the research.

2. Scope of the research

2.1. *Limitations of the research*

To start, a few remarks on the scope of the research are necessary.

Although the title of this report may seem to promise a wide scope, the actual research is more limited. The reasons for this limitation are primarily practical: cybercrime is such a multifaceted problem that an analysis of all possible aspects of cybercrime would be hard to combine with a multi-jurisdictional analysis of the legal side. Therefore a selection of three important topics and four jurisdictions was necessary. However when analysing these topics it will be necessary to also discuss two central factors in cybercrime (malware and botnets), which are also influential for many other forms of cybercrime. Thereby the relevance of this research is broader than the selected three topics would suggest.

The focus of the present research is on legal analysis. We will, however, provide a provisional factual analysis of the three selected topics of cybercrime. This analysis is fairly general and does not go into technical detail. It does not pretend completeness.

We will not address issues of competing or uncertain jurisdiction. Although this is an important practical problem, the present research focuses on what kinds of duties of care and diligence can be found, thereby giving ground for a discussion as to whether a certain amount of harmonisation might be desirable or whether specific legal measures might be effective.

In this research we will not discuss the duties of the principal offenders or criminals. It is quite clear that the principal agents act in an unlawful manner; the question here is rather whether anything can be done besides prosecuting the principal offenders. Furthermore, there are already numerous reports on cybercriminals.

We will also not investigate the legal obligations of private individuals. Obligations for private individuals may easily run into principled objections and fundamental rights. Private individuals cannot generally be held to a high level of expertise or be required to invest large amounts of time and money in order to operate fully secure computer systems. We will only examine their role in the incidence and the prevention of cybercrime, insofar as relevant to the present research.

Finally, we will not discuss the role of governments as principal actors. Mostly governments are in the same position as businesses, sometimes also as software vendors and/or ISPs, and their responsibilities are covered with the analysis for these categories. The role of governments in other respects, in particular as relates to the complicated issue of Internet governance, lies outside the scope of this research, as the primarily responsible actors for the Internet architecture are at best indirectly accountable to a few specific governments. As regards cyberespionage, this involves either acts allowed under specific state laws, or prohibited acts in which case the actors fall under the category of cybercriminals, which – as explained above – is explicitly required to be left out of this report. We will discuss only normal governance measures available to states to improve cybersecurity.

2.2. *Four jurisdictions*

The request for this research required four kinds of jurisdictions to be covered: the Netherlands, a common law jurisdiction such as England and Wales or the U.S.A., a middle-European country, and one of the BRIC countries. These groups are somewhat representative of the world-wide state of affairs. Next to the Netherlands, the following other three jurisdictions have been chosen.

- *The United States of America*. As the primary developer of the software and hardware which is used around the world, and the originator of the Internet, the present research would not be complete without covering the U.S.A. Given the fact that the U.S.A. consists of 50 States which each have their own laws, complementary to federal law, the description of U.S. law is necessarily limited and only will cover the basics, without claiming completeness. We will, however, consider particularly the laws of the state of California, as many influential and widely used software products and services are produced by companies residing in California. Ultimately the differences between state laws can be glossed over for the point of view taken here, as will become clear later on.
- *Brazil*. Brazil is a BRIC country with a developed legal system (influenced by Portugal), with relevant new developments regarding cybercrime.
- *Czech Republic*. The Czech Republic is representative of many middle-European countries in having a recent codification, influenced by European Union regulation, and a different institutional culture regarding legal interpretation and enforcement.

Taken together these jurisdictions give a fair indication of the global state of affairs as regards the subject of this research.

3. Duties of care and diligence as a general legal concept

3.1. Introduction

As requested in the invitation to tender, the report focuses on the concept of ‘zorgplichten’, translated as ‘duties of care and diligence’. As this is originally a concept from Dutch law, this paragraph will briefly explain what it entails, what its advantages are, and that it can be applied to other jurisdictions.⁵

3.2. ‘Zorgplicht’ as a legal concept in Dutch law

One of the more recent developments in Dutch law is the rise of the concept of ‘zorgplicht’, literally meaning ‘duty of care’.⁶ Following art. 1383 of the French Code Civil, Dutch private law recognised the tort of negligence in the form of a liability for faults consisting of ‘onzorgvuldigheid’ (negligence).⁷ Everyone is required to act with the ‘zorgvuldigheid’, the carefulness or diligence that is required in normal social dealings. This amounts to a ‘zorgvuldigheidsplicht’ (duty of diligence). Since the 1980’s doctrine and case law increasingly use the shorter but also apparently more demanding word ‘zorgplicht’ (duty of care), which seems to require not only diligence but also active care. Legally speaking, the ‘zorgplicht’ not only requires passive caution to avoid a tortious action on the basis of negligence, but may also necessitate more active behaviour to protect others against harm, even if the primary cause of the harm lies elsewhere. One might draw an analogy with the rise of ‘positive obligations’ under the European Convention on Human Rights.

These ‘duties of care’ extend beyond tort law. In Dutch law this extension comprises the duty of contracting parties to observe the care of a reasonable contracting party.⁸ This is somewhat analogous to the general notion of ‘diligence’ as being required in service contracts in English law, or the general ‘diligence’ required of contracting parties in Romanistic legal systems.⁹ Hence the ‘zorgplicht’ forms a bridge between contract law and tort law: it encompasses both diligence and care. ‘Zorgplichten’ were discussed in Dutch public law as well. Open norms formulated as imposing a duty of care were hoped to allow sufficient flexibility to keep up with social changes, while satisfying the principle of legality.¹⁰ Such duties of care are similar to what in other jurisdictions is called goalbased regulati-

5 A similar application for comparative research can be found in Van Eijk 2010.

6 Generally Tjong Tjin Tai 2007a, 2011.

7 See art. 1402 of the Dutch Civil Code of 1838. This was for a while interpreted restrictively (HR 10 June 1910, W. 9038 (Zutphense juffrouw)), after which the Supreme Court extended the liability on the basis of art. 1401 to include liability for acting against “de zorgvuldigheid, welke in het maatschappelijk verkeer betaamt ten aanzien van eens anders persoon of goed.” (HR 31 January 1919, W. 10365 (Lindenbaum/ Cohen)).

8 A general obligation based on the duty of good faith and fair dealing.

9 See Tjong Tjin Tai 2015 and art. 2(h) Directive 2005/29/EC, defining ‘professional diligence’.

10 See Verschuren 1990, Visser 2001, Tjong Tjin Tai 2007a: 8, Van Ommeren 2011, Timmer 2011 and 2013, and references therein.

on.¹¹ ‘Zorgplicht’ thus runs from tort law to contract law and from private law to public law, providing a unified concept to refer to what is expected of individuals. But what does such a ‘zorgplicht’ entail?

In its most basic form a ‘zorgplicht’ is formulated as a duty for a person to observe or provide care for another person or object. This care is usually defined as the care that is required in the given concrete circumstances.¹² A conceptual analysis of the notion of care goes as follows. At the basis is a moral, socially recognised duty to care for others. Such a duty need not always lead to legally enforceable obligations: only for part of those duties it does. However, it can build on pre-existing knowledge and experience in social practices, which give indications as to the actual content of such a duty. An example is the duty of a parent to care for his or her child. This duty cannot and should not be fully explicated in detailed rules. Such care is provided without having to consult strict legal requirements and demands. There are nonetheless some legal sanctions in case of gross violation of this moral duty (such as abandonment).

The advantage of such a duty of care is that it formulates directly, without any possibility of misconstruction, the actual goal of the duty, namely the promotion and protection of the interests of the object of care. The subject of the duty has to follow his judgement in order to determine what this care actually requires in specific circumstances. No further specification is necessary at the level of the rule. This does not preclude a further elaboration of the general duty to care in detailed specific obligations and duties, either in statute law, precedent, or private regulation. It should, however, be noted that the primary basis of ‘zorgplicht’ is not specifically legal but rather social and moral: individuals recognise in specific contexts a non-legal obligation to act in the interests of certain others.

This pre-legal understanding of ‘zorgplichten’ makes it possible to use these duties in a broader governance analysis, wherein the traditional legal enforcement instruments of liability and criminal prosecution can be supplemented with other measures, such as private regulation.¹³

A common criticism of such duties is that they are a denaturation of what is required of the legislator, namely to clearly specify what behaviour is required or forbidden. Experiences in Dutch law indicate that duties of care may provide an appropriate level of flexibility and certainty, provided that there is sufficient knowledge and/or prior experience in

11 Timmer 2011 and 2013.

12 Tjong Tjin Tai 2007a: Ch. 2, Ch. 4-6, s. 8.4, and Tjong Tjin Tai 2011, following a partly ethical conceptual analysis based in the ethics of care (Carol Gilligan, Joan Tronto, among others).

13 This approach bears some similarities to theoretical frameworks in which state governance is explicitly conceived in interaction with an independently norm-creating and enforcing civil society, such as the work of Amitai Etzioni. The current approach, however, is agnostic as to particular social-political philosophies and does not claim to cover the whole field of governance and society.s

social practice to allow the subjects to determine what the norm actually requires.¹⁴ It may therefore function as a useful umbrella term under which to capture a variety of behaviour that would be difficult to formulate under a more specific norm, while also stimulating the *habitus* (attitude, character) that would be required from a good citizen. The uncertainty following from such a ‘zorgplicht’ is not larger than in other relatively open norms, such as ‘reckless behaviour’.

This does not mean that ‘zorgplichten’ are a panacea. One should not expect too much by simply imposing ‘zorgplichten’ where no clear practice or moral duty exists. Furthermore, one should avoid ‘caring overload’: by imposing too many duties of care, the carer may find it impossible to meet all these duties. Taking care needs to be feasible. There needs to be some assurance or indication that the duties recognised in law can actually be followed in practice. Consequently, such duties should normally be recognised only for limited cases and objects, whereby a person can know in a specific situations whose interests he has to take into account. In particular conflicting duties of care may give rise to complications in practice.

3.2. Duties of care and diligence in other jurisdictions

The ‘zorgplicht’ as a unified combination of ‘duty of care’, professional diligence, and public goal-directed regulation is particular of Dutch law and not found in other jurisdictions.¹⁵ Nonetheless, this concept can be used as an analytic tool, provided it is realised that other jurisdictions usually apply these three distinct concepts separately. A brief analysis supports the viability of this approach.

With regard to tort law, in particular the tort of negligence, comparative research in European jurisdictions supports that most legal systems recognise that individuals are required to observe appropriate care towards the interests of others.¹⁶ The most important divergence here is whether positive duties of care are recognised, in particular whether liability for pure omissions exists.¹⁷ Other jurisdictions mostly follow either the common law approach to negligence, or a civil law approach such as the French or German system.

14 Cf. Timmer 2011 and 2013, Tjong Tjin Tai 2007a, 2011, and the more theoretical analysis of Tjong Tjin Tai 2010.

15 Although a connection between contractual obligations and tort law may be recognised as well, for example in the complicated French discussion regarding Cc 6 October 2006, case 05-13.255 (available at <<https://www.courdecassation.fr/jurisprudence/2/assemblee-pleniere/22/arret-n-9364.html>>, on which Viney 2008: nr. 215-3) that recognised that a third party to a contract may claim a tort on the basis of violation of a contractual obligation.

16 Van Dam 2013: nr. 805, and Von Bar 2009: art. 3:102 and commentary, which has been adopted in the European art. VI.-3:102 Draft Common Frame of Reference.

17 In most civil law countries this is recognised, while common law countries are much less inclined to accept liability for pure omissions. See Smits 2000, Kortmann 2005, Van Dam 2013: nr. 1701-1703.

With regard to contract law, again most European systems assume to a certain extent that parties have to perform with due care and skill or using professional diligence.¹⁸ In civil law countries this is often discussed in connection with the notion of good faith and fair dealing,¹⁹ although this notion is not universally recognised.²⁰ Outside of Europe, again most jurisdictions adopt the more formal common law approach, or the civil law approach wherein the care of a good debtor is as a matter of course recognised.

In chapter 5 we will show that all jurisdictions studied here do recognise such duties of care in tort and duties of diligence in contract law. This follows the general contours of what has been described here as duties of care and diligence. The exact extent of these obligations may differ, but the general thrust – in that some care must be shown towards another's interests – is widely accepted. Even if no unified concept is recognised, we can use a unified concept at least for research purposes in order to categorise and systematise the findings in various jurisdictions. In order to avoid having to use the Dutch word 'zorgplicht', and to avoid misunderstandings with using the literal translation of 'duty of care'²¹ (given the specific meaning this has in English tort law), we use the broader phrase '*duties of care and diligence*'.

3.3. Duties of care and diligence as an analytic framework

Given the effort it takes to make the concept of 'duties of care and diligence' understood in a global context one might wonder why we use this as the basis of the present analysis. The answer is that it has several advantages.²²

First of all, the general ethical and social background of the concepts of care and diligence provides a focus first on what is to be done, i.e. the actions or measures that we would like or expect. Only after that we may address the questions of possible remedies or enforcement. In law there is a tendency to focus on whether one has a ground for action in court, whereby one abstracts from what actions or measures would be useful. In the present report we explicitly want to discuss possible beneficial actions in general and only then investigate whether these actions are mandatory under the law of various jurisdictions and if so, whether they are enforced.

Secondly, the concept of duties of care and diligence is not necessarily limited to one subdivision of law. It may be applied equally to private and public law. It is, therefore, eminently suitable for a more encompassing governance-based view in which various legal

18 Tjong Tjin Tai 2015 for service contracts, with some indications as to general contract law.

19 Cf. art. I.-1:103 Draft Common Frame of Reference.

20 See the comparative work Zimmermann & Whittaker 2000.

21 In Van Eijck 2010 'duty of care' could be used as the report was concerned with extra-contractual obligations

22 Cf. Tjong Tjin Tai 2011.

remedies and actions are considered as independent interacting elements that may have the desired social effects. Furthermore, as the concept is not purely legal, it may easily take into account non-legal norms as well.

Third, the concept of duties of care and diligence focuses on the person or object on whose behalf one acts. The discussion on which obligations are part of such duties thereby does not lose sight of whether the obligatory actions actually benefit the object of the assumed care.

Fourth, duties of care and diligence are typically not laid down in advance in abstracto. Rather, the precise obligations that flow from these duties by necessity must be determined in the specific circumstances of the case, with a view to the object of care. This provides an inherent flexibility to adapt to changing circumstances, in particular to new threats such as cybercrime. Insofar as positive law does not provide clear indications as to which obligations exist to combat cybercrime, duties of care and diligence may provide a provisional albeit weak justification for assuming certain obligations.

Fifth, duties of care and diligence are suitable for a networked environment where events involve many parties all of whom are, theoretically, in a position to prevent the event from occurring. When discussing notions of responsibility and liability there is a tendency to focus on the primary agent, leaving the possibility of other agents to take preventative action out of consideration. One should distinguish between the responsibility of the primary agent and the lesser responsibilities of others (as can be done by distinguishing between primary care and subsidiary care). However, duties of care and diligence may overlap: the fact that one person can and should primarily take preventive action does not mean that another person who is in the position to do something has no duties at all. An analysis along these lines may provide a more complete preventive structure than one built on strictly separate and exclusive individual responsibilities. Care and diligence allow for shared responsibility, while postponing the issue of ultimate liability.

Regardless of these advantages, we should clarify at the outset that duties of care and diligence may function well only in a specific regulatory context.²³ Such duties assume a positive, willing attitude of the parties concerned. This attitude justifies the necessary trust and faith in the actions of parties: even where there are different opinions of what would be the best action, this does not mean that alternative opinions are completely wrong. Duties of care and diligence are not maximising, merely satisficing: a sufficient level of care is enough. Even where parties intend the best result, outside observers should not find fault if this ideal is not arrived at. Incidentally, it follows that duties of care and diligence are no guarantee that nothing ever goes wrong. Only where a party acted decidedly below a sufficient level of care can we come to the judgement that there has not been a real effort

23 Cf. Tjong Tjin Tai 2011.

to provide good care. Hence legal liability is a sanction only for fairly extreme shortfalls in care. Given the presumed trust in parties, we should assume the existence of a thriving caring practice, in which standards of good care can arise. Such a practice requires communication between others in similar situations, in order that people can benefit from each other's experiences.

Such an ideal caring practice may not always exist. It is possible, in the absence of the necessary willing attitude, to add external incentives such as liability or reputational damage. Such incentives may lead to establishing safety rules or hiring compliance officers, which may positively influence a corporate culture. Even then, duties of care and diligence require a hands-off approach or attitude of forbearance, where guidance is mostly provided through incidental supervisory interference or court intervention, without detailed government regulation. Too detailed regulation signals that parties bear no responsibility for developing good practices, and may lead to an attitude of doing no more than the rules proscribe. This undercuts the benefits of duties of care and diligence, in particular the possibility of rapid incorporation of localised experience and expertise, tailored to individual relationships. Centralised standard setting will unavoidably be too general and too late.

3.4. Conclusion

Duties of care and diligence may therefore, if applied correctly, constitute an effective and efficient form of governance. The question is if this concept may help to address the problem of cybercrime: where and how can we break the chain of events that leads to cybercrime?

4. Causes and manifestations of cybercrime

4.1. Introduction

Cybercrime has become an important threat to the security and safety of Internet usage.²⁴ The risk of becoming a victim of cybercrime has obliged individuals and corporations to take many safety measures that would otherwise have been unnecessary, while the consequences of cybercrime activity can be enormous, both in terms of individual loss of money, privacy and confidence as in terms of corporate losses and state damage. There appears to be a race between increasingly sophisticated criminals and those who try to prevent cybercrime, and it is not at all clear that the latter group is in the lead.

In order to keep the present report manageable the focus will be on three topics. First of all, we concentrate on two specific forms of cybercrime: ransomware and DDoS attacks. These are topical and representative of a number of related forms of cybercrime. We will further pay particular attention to one specific element of the causal chain that leads to cybercrime: the lack of security of hardware and/or software.

A proper description of these three topics, however, also requires an investigation of two central elements in the causal chain to these forms of cybercrime: malware and botnets. The advantage of also investigating these two phenomena is that many other forms of cybercrime also require the presence and control of malware and/or botnets. The present analysis is therefore also relevant for these other forms of cybercrime.²⁵

We begin with a case example to illustrate how cybercrime may spread, and which actors may be involved (s. 4.2). This is followed by an introduction of the main actors relevant to the current research, and the manner in which these will be referred to (s. 4.3). In order to keep the research manageable, some simplifications are made. Sections 4.4 through 4.6 contain an analysis of factual causes and contributing factors to the topics of cybercrime. The analysis is divided into three parts: primary causes of infection (s. 4.4), malware and botnets, being central factors and crimes (s. 4.5), and two specific forms of cybercrime, ransomware and DDoS attacks (s. 4.6). In section 4.7 we summarize the list of relevant actors and possible preventive actions they might take. We will end with a conclusion (s. 4.8).

4.2. A case example

To introduce the problems that are the focus of this report, we will first discuss a case example.

Ann receives an e-mail on her computer, which appears to be sent by her bank. The e-mail

24 See OECD 2008, ITU 2011, UNODC 2013 (draft report), also Van der Meulen & Lodder 2014.

25 However, it remains possible that for a specific form of cybercrime there exist other preventive measures than those discussed here, as such measures rely on features particular for this form of cybercrime. Hence even if malware is necessary for such a cybercrime, this report may ignore such other precautions even if they would be feasible.

warns her of a security problem and urges her to look for further information at the Internet address provided by a link in the e-mail. She clicks on the link, which opens her Internet browser. However, the browser refuses to open the address, instead warning her that the address has been suspected of containing malware. Thus warned, she recognises that the e-mail is in fact a forgery.

Ann continues browsing for information, and comes across a general discussion forum which also shows ads at the top of the page. Without knowing it, this ad contains a script that makes use of a vulnerability in her software.²⁶ Although she has regularly updated her software, the vulnerability used was not patched yet. Through the execution of the script a malware program is installed on her computer. Although her computer is supplied with an anti-virus program, the program does not detect the malware because it is a new form of malware which has not yet been recognised by the security community.

The malware executes automatically at start-up of the computer and is unobtrusive, so Ann doesn't notice anything in her computer's behaviour. The malware occasionally communicates through her Internet connection to the criminal who is behind the malware. This communication passes through the firewall installed on Ann's computer. Originally the firewall was configured to be much stricter in monitoring suspicious traffic, but that interfered with some legitimate programs that Ann used. She therefore asked a befriended computer expert to change the settings to a less strict (and thereby less secure) level.

The malware monitors Ann's Internet behaviour, investigates the data on her computer, copies and transmits her e-mail address book, Internet login names and passwords to the criminal and occasionally sends out spam. The malware could also have deleted data, but that might have alerted Ann that there is something amiss, hence the criminal at present refrains from such actions. Deleting data would have been a serious loss to Ann as she doesn't keep consistent backups.

The criminal behind the malware has been successful in infecting thousands of user computers, both private computers and computers used in businesses. He has thereby formed a so-called *botnet*: a large network of 'bots', programs that are fully under his control and command (see s. 4.6.3). Besides using the botnet for further infections, the 'botnet herder', as such a criminal is sometimes called, rents out the botnet for criminal purposes. He is paid occasionally to send spam e-mails.

Ann's Internet Service Provider (ISP) is by now aware of the existence of the kind of malware that has infected Ann's computer. The security officer of the ISP considers whether malware infections could be determined through an investigation of the origin of a recent flood of spam mail. However, he decides against it. First of all, the origin may be masked by

²⁶ This might be in the browser, or in a browser extension or plugin such as Flash player. For the example it doesn't matter where exactly the vulnerability is located.

Internet proxies which hide the actual sender of mail. Hence an examination of the received e-mails may not work. Secondly, to determine whether a client of the ISP sends spam requires in-depth examination of private Internet traffic. Such 'deep packet inspection' may be considered to violate privacy. An examination of the emails that are being sent out is therefore not a viable option either. Thirdly, even if the actual senders are identified, it may be too complicated for them to clean their computers from the malware. Even though the ISP contract contains a clause allowing the ISP to cut off the Internet connection for 'infected' computers, it would be bad publicity if they would actually take such action on a large scale. As a result, the ISP refrains from this effort.

One day the bot herder is asked to perform a DDoS attack²⁷ on the website of a large multinational company. He instructs all the 'bots' in the botnet to send Internet communication requests to the attacked website. The immense volume of requests leads to overload of the servers, because of which the website becomes unreachable. Ann's computer plays a tiny role in the attack, sending out hundreds of requests per minute, being one of thousands of similar computers doing so.

The multinational being attacked is aware of the attack but finds it difficult to take appropriate measures, as the DDoS requests are not easy to distinguish from legitimate requests. The ISPs through which the communication requests of the botnet passes help the police and a private security service provider in trying to detect the botnet herder. However, the forensic investigation takes much longer than the attack lasts.

Only several weeks later some Internet news websites mention an arrest made of the individual suspected of being the botnet herder. Ann happens to surf to such a website but quickly scrolls over this news item, as this doesn't interest her.

4.3. Actors involved in the prevention of cybercrime

As the example already shows, there are numerous parties or actors involved in the prevention of cybercrime. The various roles they fulfil may differ, and these roles may have different names in various contexts. In order to avoid misunderstandings and in order to keep the discussion manageable, we will operate with a limited set of actors and roles. In this paragraph we will explain which actors are investigated primarily and why this selection makes sense.

There are three actors that are central to our analysis:

- **Internet service providers (ISPs).** This refers to businesses or non-profit organisations that provide specific services central to the operation of the Internet. In particular, ISPs are understood to encompass hosting providers (which host websites and make the content available through the Internet), access providers

²⁷ See s. 4.6.3.

(who provide end users Internet access), as well as other content and service providers such as search engines (e.g. Google), trading platforms (such as eBay), social media (e.g. Twitter, Facebook).²⁸ These organisations store and transmit Internet traffic and thereby are in a position to notice what is occurring, and to block undesirable content.²⁹ The ISP may, simply put, have a *responsibility for Internet traffic*.

- **Software vendors.** By this we mean individuals or organisations which develop and publicise³⁰ mass-market software (possibly besides other IT products). Examples are companies such as Microsoft, Apple,³¹ Google,³² Adobe, Namco, Sony, Symantec. The software vendor is meant to denote the party or parties *responsible for the quality of mass-market software*.
- **Businesses.** With this simple term we mean businesses other than the previous two categories: companies who have a business in a different market, are active on the Internet and use software purely as a means to facilitate their core business.³³ A more precise name would be ‘non-software, non-Internet businesses’, but that would be unwieldy. With businesses we mean to identify the organisations *responsible for security and availability of their own IT*.

By focusing on these three actors and the roles they fulfil we cover the most important areas where duties of care and diligence to prevent cybercrime may exist. This follows the practice in earlier reports on cybercrime. Although ‘pure’ types or roles may not always exist, this is a justified approach for descriptive and analytic purposes.³⁴ An organisation which does not strictly fall under a single role can be analysed as fulfilling several of these roles in different contexts. For example, Google is an ISP (as operating a search engine), a software vendor (by developing and making public the Android mobile OS and the Chrome browser), and a business (where it provides other services and products that may be marketed and need their own security). An ISP may become the victim of a software

28 As is recognised in EU case law, see s. 5.2.2.3.

29 Extensively on the role of ISPs in preventing cybercrime: Peterson, Segal & Eonas 2014, also Lichtman & Posner 2004 and 2006, see further references in s. 5.3.2.4.

30 This can be by direct sale or by making it freely available for download, or through intermediaries.

31 Which mainly is a hardware company but also sells software such as OS X and related programs.

32 Which is mainly an IT service provider, but also creates and makes available software such as the Android OS for mobile phones.

33 We will occasionally look at sector-specific rules, but mostly will discuss businesses in general.

34 In effect we operate with ‘ideal types’ following the sociologist Max Weber.

vulnerability in the same way as a general business.³⁵ It would not make sense to create specific categories for such organisations fulfilling multiple roles, since an investigation of each of the separate roles also covers (as far as this research is concerned) the organisation as a whole.

To support this position, we will first devote some additional remarks to the concept of ‘software vendor’. Subsequently we will justify the choice for not separately discussing IT service providers.

Our reason for working with a concept of ‘software vendor’ is to target the entity that is responsible as a matter of law, on the basis of contract or tort, for the quality of the mass-market software made available to the public. Given the complex environment in which software is produced and marketed it is next to impossible to provide a precise and complete workable definition.³⁶ Software may, for example, be developed inhouse, but usually is also developed with the help of freelance programmers or external IT developers. Software may be marketed and made available through the use of a variety of marketing channels, such as App stores³⁷ and other intermediaries,³⁸ including software distributors and stores (physical or Internet-based), in which case the store is legally speaking the vendor.

However, ‘vendor’ appears preferable to ‘developer’ as ‘developer’ is associated more with the individual developers than the responsible integrating company. The analogy is rather with ‘manufacturer’ in for example the automobile industry, but ‘software manufacturer’ is not a common term. With ‘vendor’ we follow the usage in other reports.³⁹ ‘Software company’ might be considered as an alternative, however, this may lead to confusion as it may also be used to denote an IT service provider who does not create mass-market software.

Although the term ‘vendor’ suggests that the software is sold, this is not a requirement for the definition used here. We specifically want to include open source software and other software made available for free (freeware).

We focus on mass-market software rather than bespoke or tailor-made software, because the former is a structural cause of mass infections of computers. Moreover, if the

35 For example a vulnerability (the Shellshock bug) in the Bash shell on Unix systems, used on many web-servers, could be exploited with a carefully crafted http-request, see <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169> and <http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/>

36 Note also that the companies used as illustration are not the actual legal entities, as specific software may very well be marketed or developed by a subsidiary, which may even be different in various jurisdictions.

37 The Apple App Store, Google Play store.

38 For example Steam (for computer games), Sourceforge (for open source software), Softonic.

39 Such as the OECD 2008 report.

quality of software development of mass-market software is raised, this may be expected to have beneficial effects as to the development of bespoke software. There are measures to improve the security of mass-market software, such as bounty programs, which are more costly and less effective for bespoke software (as these would at best result in finding single vulnerabilities with the individual business using this software).

We do not specifically address Software as a Service (SaaS), as that is only a specific way in which software is made available to a business. If a security breach is made possible by a vulnerability in software made available as a service, it doesn't matter that the software was used in a specific contractual and organisational constellation. The same analysis as to the existence of vulnerabilities (in the code or in the configuration) applies as when the software would reside on a computer of the principal.

Furthermore, software may also be sold as part of hardware.⁴⁰ The term 'software vendor' is agnostic to the way in which software is provided, even though the seller of hardware which includes software will not be called a software vendor in practice.

We do not discuss *IT service providers* as a separate type of actor. Many individuals and organisations provide IT services to others, usually on a commercial basis. These services may encompass software development, communication services, security services, outsourcing, support and maintenance. Business and software companies may hire IT service providers for a variety of reasons, i.e. to develop bespoke software or to help in configuring mass-market software such as SAP.

Our primary reason for not considering IT service providers as a separate type of actor is that the relevant parts of their contribution are covered by the organisations that hire them (the principals): ISPs, software vendors, and businesses. The IT service provider is hired to fulfil a specific task. Insofar as the IT service provider thereby would have a specific responsibility towards third parties, this is one that the principal would have had himself. Hence by discussing the role of the principals, we also cover any responsibility of independent IT service providers to third parties. Furthermore, an IT service provider can only take actions that the principal could also take himself. Many large organisations have an internal IT department, which performs the same function an external IT service provider would otherwise fulfil. Conversely, a company could outsource its IT to an external service provider. These differences in organisation do not matter for the broad legal analysis required here.

⁴⁰ For example Samsung may deliver mobile phones with software installed (both third party and proprietary Samsung software).

One complication is that in some cases the principal might no longer be liable after ‘outsourcing’ his responsibility. This leads to the complicated issue of liability for independent auxiliaries and the related (common law) topic of ‘non-delegable duties’. However, the focus on duties of care and diligence can abstract from this legal issue: if we can establish whether the principal would have such a duty, that is sufficient, regardless of whether the principal might on occasion be relieved of liability by transferring the responsibility to the service provider.

A second point where this distinction could be relevant is when discussing a solution to improve the level of expertise of IT service providers in general. We will touch on that possibility briefly (s. 8.3). It should be noted that in this regard we distinguish between IT service providers as the organisations that contractually agree to provide services, or the individual professionals within those organisations who actually perform the services. In the analogous situation of lawyers, which in many countries is a strongly regulated profession, the rules of professional ethics and the requirements for professional education are aimed principally at the individuals, and only to a lesser extent at the organisations by which they are employed. Therefore, professionalization of the IT sector would involve educating IT professionals, irrespective of whether they are employed by businesses or by independent IT service providers. This therefore supports the argument that there is no need for considering IT service providers as a separate actor.

A third point of note is that IT service providers may develop bespoke software or configure mass-market software on behalf of a business, and in the course of this activity may make errors that leave the system open for unlawful intrusion. Although this may lead to security breaches, we can consider these as falling under the heading of ‘user security awareness’ (s. 4.4.2): these are not structural failings that call for a general solution, but rather incidents that may be abused and can be countered by improving security awareness – in this case the awareness of the IT service provider hired by the business. The same errors could be committed by an internal IT department, which would then clearly be the responsibility of the business. If personal data of customers has been leaked, the business cannot disclaim responsibility by pointing out that the IT service provider made the actual error. Note that a business can, if necessary, sue the external service provider to recover costs or losses incurred because of its negligence (such as the damages resulting from liability for the security breach towards the consumer).

4.4. Primary causes of security breaches

4.4.1. Introduction

As mentioned above, cybercrime is a multifaceted phenomenon which takes on many forms. However, some features are common to the spread of cybercrime. We will discuss

two parts of the causal chain that leads to cybercrime: lack of security awareness on the side of the user, and lack of software security. These are the principal causes of malware infection,⁴¹ by allowing security breaches through vulnerabilities in the system.⁴²

4.4.2. Lack of user security awareness

Many forms of cybercrime involve a security breach of a computer. Such a security breach may be caused without any user contribution, because software contains a bug (or *exploit*) that allows a criminal unauthorised access to the computer (see s. 4.4.3). However, a security breach may also occur because the user has neglected to take sufficient security measures, or has involuntarily or deliberately overridden existing security measures.⁴³ To illustrate the importance of even minimal security measures: if no firewall is installed, a computer can become infected within minutes after being connected to the Internet!⁴⁴

As is well known, security of computers with Internet connectivity may be improved by installing anti-virus software, firewalls, and specific security measures that nowadays become more common in software (such as explicit user permission for execution of downloaded programs and warnings for websites known to contain malware). In practice, though, there is a high number of computer users that do not adhere to best practices in security. This may be due to any of a number of causes.

The cause may be simply a lack of computer literacy: a user may not actually know about such security measures, or may lack the knowledge to install or use such software.

⁴¹ See on malware s. 4.3.2. Cf. OECD 2008: 12, on the causes ('propagation vectors') of malware infection.

⁴² See also Pinkney 2002.

⁴³ See also Chong 2013c.

⁴⁴ Mueller 2006. An open Internet connection can be abused by sending communication requests that exploit bugs in the computer software, through which malware may be installed without any active use of the Internet by the computer user.

A user may be security aware, but may lack the money, time, or energy to actually take the appropriate measures. If the user has formally taken such measures, he may have installed them incorrectly, for example by forgetting to configure a firewall with the right settings so it is inoperable or to have it run automatically at start up of the computer.⁴⁵ He may forget to update the software. These mistakes can be illustrated by an analogy with the off-line world: a home owner may not know that he should have a lock on his door, he may lack the money to have a lock installed, or he may forget to actually lock the door.

Furthermore the user may bypass or override the default security measures. When inserting a USB-stick a user may choose to stop the virus scanner because it takes too long. A user may choose to open a Word document received in an e-mail attachment with macros allowed. This creates security risks, but these risks may be acceptable if the document is from a trusted source. However, it is possible that the source is compromised: the mail may be infected with malware from a friend's computer. A user may receive genuine-looking e-mail containing hyperlinks, which may infect his computer if he clicks on the link. A user may, while web surfing, come across websites that contain malware,⁴⁶ which may exploit bugs in his web browser whereby his computer may be infected without his knowledge. Furthermore, a website may open a pop-up window that looks as if genuine software asks for a security update:⁴⁷ if the user believes that this is a genuine requests he may subsequently download and execute malware. These examples are more sophisticated and may easily fool a gullible or unsuspecting user, as well as a suspicious user with insufficient computer expertise (to distinguish real update requests from fake ones). In the earlier analogy this is like a person who opens the door for an unknown individual, or opens the door for someone who looks like a police agent, or opens the door for someone who looks like a friend.

Another category of cases are those where users deliberately find and execute software from non-official sources. This may be perfectly legitimate and safe, for example with well-known open source software like the Linux operating system. It may also be of uncertain safety, as when downloading software from an individual developer without a track record. It may also be rather risky, as when downloading software found at websites that offer illegal copies of commercial software.⁴⁸ Similarly, a user may choose to deliberately bypass

45 Or also forget to change the default password, which used to be a common mistake with private WiFi routers.

46 This may be as part of the website itself, or be present in an advertisement displayed on the website (which often is outside the control of the website owner).

47 This is an example of 'drive-by download', which is a known infection method of malware, see <http://arstechnica.com/security/2004/11/malware/5/>

48 These copies may have been deliberately infected with malware and placed at such websites in order to spread malware.

the security features of his hardware/software combination in order to allow download and execution of pirated copies of games or other software.⁴⁹

Finally there are non-technical ways in which security breaches may occur. Social engineering is one primary way:⁵⁰ a hacker uses his knowledge of social interaction to guess passwords, or to convince a user (through computer-mediated communication) to give his passwords or otherwise provide access to his computer. This is usually done by posing as an authoritative person (police, bank officer, IT support etc.).

Proper computer education may limit the risks associated with such actions and attempts by instilling a general suspicion that makes the user double-check things with independent sources, avoid malicious hyperlinks by going directly to the official website of the institution or vendor, and keep his password secret no matter how trustworthy another person seems. Raising user security awareness has been advocated frequently.⁵¹

Raising user security awareness is not a general solution, as correct installation and use of required security measures may well be too complicated for most individuals.⁵² Another option would be to disallow unlicensed buying, installing and Internet use of computers by individuals.⁵³ However, this option is undesirable (if not politically impossible to realise), as it is contrary to a basic right to Internet connectivity.⁵⁴ It must therefore be regarded as an unavoidable fact that large numbers of computers are insufficiently secure, even in the absence of software vulnerabilities.

Although we do not focus on private users, the above analysis is relevant as it lists actions that *businesses* may take to enhance the security of their IT. The argument that lay users lack the expertise for taking proper security measures does not hold for business users, who in the course of their business may be required to have or hire the requisite expertise. Without repeating the detailed actions mentioned before, we can conclude the following.

49 Called 'jailbreaking'; it involves installing a tailor-made operating system on the device. Cf. https://en.wikipedia.org/wiki/IOS_jailbreaking. This may have perfectly legitimate reasons, but is also used to circumvent the prohibitions on illegal software.

50 Luo and Liao 2007: 199.

51 For example OECD 2008: 52, ENISA 2011: 124. Barnes 2004: 328-329 even advocates small penalties for users that fail to take appropriate steps (albeit realising the enforcement problems involved). A related measure is to assume contributory negligence (for failing to take appropriate measures) in cases where users claim damage because of cybercrime. As this is not the subject of this research, we will not discuss the desirability of user penalties.

52 This is not meant to be derogatory towards lay users. The fact is that for example properly installing, configuring and using a firewall ideally requires extensive knowledge about technical details (for knowing which channels to block in principle and to allow in principle, knowing what it means when program X wants to use channel Y) which cannot be required from common users.

53 Thereby applying restrictions in spread and use as are common for example with medicinal drugs, of which the sale and distribution is in the hands of professional groups, or with automobiles, of which installation and repair is mostly (but not completely) in the hands of tightly organised distribution chains.

54 See s. 7.4.

Businesses can take a variety of preventive actions to prevent infections by malware and other security breaches. This requires significant effort and expertise, and has to be kept up to date.

4.4.3. *Security of hardware and software*

A second major contributing factor to security breaches is the existence of vulnerabilities in software.⁵⁵ This involves both commercial software, such as the software used for creating and running websites (in particular webserver and Content Management System (CMS) software), as well as consumer software used to access the Internet (in particular web browsers and plugins).

Vulnerabilities in the software may be due to mistakes in the programming. Examples are a lack of input bounds checking (too large inputs may lead to a so-called *buffer overflow*, whereby the input overwrites program data and thereby may reach parts of the system that should not be reached)⁵⁶ and SQL injection or script injection bugs (data input is interpreted as SQL or script code, thereby allowing the criminal to execute his own code on the targeted computer).

Such vulnerabilities are often called *bugs*. ‘Bug’ could be defined as that software behaves incorrectly, which would mean that correct software would not contain any bugs. However, bugs are usually also meant to refer to software that behaves in unintended ways, which may be the case even if the software strictly follows the specifications (i.e. behaves formally correct). Bugs may relate to the desired primary functionality, but the existence of a vulnerability is also one kind of bug, to wit a security bug. Hereafter we will speak of both vulnerabilities and bugs, whereby the context should make clear whether we mean bugs in general or security bugs (vulnerabilities).

Software vendors desire to avoid bugs. The effort to avoid bugs can be qualified as greater diligence in developing software. However, it is difficult to explicate what such diligence actually requires in practice, not only because it is not fully clear which efforts can actually reduce the number of bugs, but also because there are disincentives at work. Generally speaking the problem of the widespread existence of insecure software seems to be due to the following.⁵⁷

As is generally acknowledged, most modern software is highly complex and of mas-

55 We describe general trends in the software industry, while acknowledging the existence of significant efforts by many companies. Furthermore, the following text does not aim at description of a single jurisdiction, but rather at the global software industry.

56 Or the converse, that the attacker may request an overly large output string, as was the case in the HeartBleed bug (see below).

57 See also Warner & Sloan 2012 and the New Republic article series by Chong (2013a-2013d), and OECD 2009: 109-122, particularly 116-121.

sive size. Software is hardly ever created from scratch, and almost never in machine code or assembly language. This means that software is developed by building on previous programs: by compilers and interpreters that translate high-level programs into local machine instructions, and by using building blocks created by other developers, which may be called ‘libraries’, ‘API’s’, and so on. Even if we only look at the software code that is completely created by a company in-house, the total source code may easily encompass millions of lines of code. The sheer size of software makes it practically impossible to guarantee the correctness of the software and the absence of bugs.⁵⁸ It should be noted that, depending on the definitions used, correctness and bug-free are not identical. Correct software may be seen as software that provides the correct output with the correct input (functionally is correct), while bug-free software does not exhibit undesirable side-effects. Correct software may therefore contain bugs.⁵⁹

The presence of bugs that lead to security breaches is undesirable for the software industry. Software developers naturally wish to avoid bugs. However, in practice there is a strong drive to be first to release a product on the market:⁶⁰ it is better to market a relatively buggy program but be the first program of its kind that consumers buy, than market a bug-free program that consumers will not buy because they already have a similar product. Although consumers complain of buggy software, these complaints are usually aimed primarily at errors in the principal functionality. Hence testing may focus too much on functionality and too little on security.⁶¹

Could a change in methodologies provide a solution? There have been numerous efforts at creating software development methodologies that prove the correctness of programs. The computer language Ada was designed to allow only correct programming. However, in practice it is found that such methodologies and languages are too restrictive.

58 This may be partly due to an insufficient attitude, partly to human fallibility. It has been estimated that (even) experienced software engineers normally inject 100 or more defects per 1000 lines of source code (James E. Bednar, available at http://www.inf.ed.ac.uk/teaching/courses/seoc2/2004_2005/slides/quality.pdf, referring to W.S. Humphrey, *A Discipline for Software Engineering*, Reading, MA: Addison-Wesley 2002). W.S. Humphrey also pointed to the importance of attitude to reduce this number (<http://www.sei.cmu.edu/library/abstracts/news-at-sei/wattsnew20043.cfm>). See also <http://www.sei.cmu.edu/library/abstracts/news-at-sei/wattsmar99.cfm> about the difficulty of actually removing bugs (or defects, as Humphrey prefers) by testing.

59 An example may be a program that does calculate mathematical sums correctly, but which, when confronted with a specific, mathematically meaningless sequence, may allow the user super-user access to the computer.

60 Cf. Warner & Sloan 2012, Barnes 2004: 288-302, also Pinkney 2002: 65-58, Chong 2013c referring to <http://www.schneier.com/essay-025.html>.

61 For example the use of alpha testers and beta testers for game software detects primarily errors while playing and will not uncover security flaws.

Programmers prefer less secure but easier to handle languages like C and its derivatives like C++ and C#, Java, Python, SQL, Visual Basic, and languages particular to Internet software such as PHP, Javascript, and Ruby. Even insofar as functionally correct (and bug-free) programming is indeed humanly possible, the demands of software development economics are hard to combine with following the rigour and strictness that theoretically would be required, as that would demand excessive investments of people, time and money. The popularity of Agile development methods (which allow rapid delivery of functionality through iterative development)⁶² may further increase the trend towards functionality at the expense of security.

That does not mean that no methodology is used at all, or that methodologies are never used in practice. The widespread use of object-oriented programming languages and type checking is in itself an improvement over functional programming or the even older practice of code with GOTOs.⁶³ Another example is the rise of ‘security by design’, whereby systems are from the ground up designed for being secure. Proper methodologies should at least reduce the number of bugs. One aspect of methodology is the use of a testing phase. However, testing may often aim at functionality, rather than security: tests may focus on whether the software does what it should do in the circumstances for which it is designed.⁶⁴ Tests are not always examining whether the software is robust against attempts to break the software.

It appears therefore that regardless of the correctness of software, software development might be improved from the point of view of cybersecurity by methodically looking at the prevention of vulnerabilities. Standards may be set to look for common errors, such as buffer errors, incorrect link administration, and script injection. Insofar as human testing of program behaviour is insufficient, the source code may be inspected (code inspection). This can be done by human inspection, or with the aid of automated code review tools that could detect certain kinds of errors in the source code for common development languages.⁶⁵ Most vulnerabilities seem to derive from specific, wellknown types of errors.⁶⁶

62 Creating a demo system that is improved in each iteration to add functionality and remove bugs; the disadvantage is that this is geared towards providing functionality, while as such having little regard for security, except if specific security tests are added to the process.

63 However, the theoretically strict demands of type checking and object oriented programming are in practice often relaxed in order to enhance ease of programming and therefore programmer productivity.

64 For example the ISO/IEC 9126 seems to be aimed primarily at functionality and concomitant requirements not at robustness, even though arguably robustness might be made part of functionality.

65 A quick search for automated code review provides numerous examples. See also the overview in Gary McGraw, ‘Automated Code Review Tools for Security’, Computer 2008, p. 92-95 (with references to further literature). See also s. 6.6.3.

66 It should however be noted that it may be impossible to automatically detect all or even most actual vulnerabilities, as these may take very different forms. Recognising all possible forms may be so complicated that a tool would take an inordinate amount of time to process a reasonable sized piece of source code.

In the industry one can find numerous examples of secure coding practices⁶⁷ or secure coding standards.⁶⁸ However, these standards have clearly been unable on their own to eradicate all vulnerabilities,⁶⁹ which shows that they are either inadequate on their own, or not implemented correctly. Simply adopting a standard that is claimed to promote secure development doesn't make the software secure, just as adopting a code that bank officials are to act ethical doesn't ensure that they actually comply with the code. Standards may be too vague, miss out new kinds of vulnerabilities, or may be difficult in other ways to apply in practice in an *effective* manner.⁷⁰ Besides standards, the attitude of developers would have to include awareness of and attention to security.⁷¹ There is not a single, industry-wide, set of generally accepted standards that gives clear, easily applicable and effective rules to avoid vulnerabilities.⁷² Development of such standards is furthermore hindered because companies do not generally publicly make clear what actually caused specific vulnerabilities and how this could have been prevented.⁷³

This is not to say that companies are not doing what they can. On the contrary, many companies are already devoting significant resources to improving security. Microsoft, for example, has for years been promoting standards and policies in company and with outside contractors aimed at increasing software security.⁷⁴ Assumedly these policies have also been discussed and implemented within the company, allowing internal learning

67 Just to name a few random examples: SafeCode, Fundamental Practices for Secure Software Development, 2nd ed. 2011 (http://www.safecode.org/publication/SAFECode_Dev_Practices0211.pdf), CERT (Carnegie Mellon University) Coding standards: Top 10 Secure Coding Practices (<https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices>), https://www.isc2.org/uploadedfiles/isc2_public_content/certification_programs/csslp/isc2_wpiv.pdf.

68 Such as R.C. Seacord, The CERT C Secure Coding Standard, Boston: Addison-Wesley 2008 (and for other standards <https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards>), Microsoft public Secure Coding Guidelines for the .NET framework ([http://msdn.microsoft.com/en-us/library/d55zxx87\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/d55zxx87(v=vs.90).aspx)).

69 As proven by the numerous vulnerabilities still found.

70 Simply verbally adopting a practice is not sufficient; the practice should actually be followed at all times, which may be hard due to human forgetfulness, time pressures, simple oversights and errors. Hence the standard or practice has to be embedded in the whole organisation, as for example appears to be the aim of ISO/IEC 27001, ISO/IEC 27014 (regarding governance of information security), ISO/IEC 27018 (regarding protection of personally identifiable information), and ISO/IEC 27034 (application security), or (to name a random example) <http://www.bsimm.com/online/>.

71 As for example advocated by Watts S. Humphrey (PSP: A Self-Improvement Process for Software Engineers, Boston: Addison-Wesley 2005).

72 In regulated sectors such as the medical or legal sector there are some widely accepted, clear, relatively specific guidelines (such as informed consent, prohibition of conflict of interest) which at least provide some concrete guidance. Admittedly such guidelines again do not manage to fully prevent professional errors or crimes.

73 There may of course be good reasons for not doing so, such as protection of trade secrets. We only point out the lack of such discussion. See also s. 8.3 on the relevance of communication.

74 See for example the Microsoft Security Development Lifecycle (<https://www.microsoft.com/security/sdl/default.aspx>) from 2002, which became mandatory policy in 2004.

processes. Furthermore, Microsoft adopted a program for sharing knowledge and best practices regarding security.⁷⁵ Similar analysis can be made of many other large software vendors. However, it should be noted that even such extensive efforts do not yet manage to completely eradicate all vulnerabilities.⁷⁶ One can either conclude that these extensive efforts are still insufficient and more should be done (in which case the question is whether additional measures and/or incentive are required, which will be discussed in the remainder of this report), or that the present level of vulnerabilities are a fact of life which is to be accepted.⁷⁷ In the latter case, of course, the following recommendations can be disregarded with respect to the companies who actually do take such a level of effort.

Furthermore, the existence of companies that spend much effort to produce secure software does not negate the existence of companies that may be lacking in such efforts. For those companies the remainder of the report, discussing further incentives, is still relevant.

Vulnerabilities are not by their very nature impossible to discover. Indeed, the fact that such bugs are exploited by criminals proves that they *are* discoverable, only it is often criminals who first discover them. This shows the truth of the economic analysis in the OECD 2008 report: criminals have strong commercial incentives to look for vulnerabilities, while software companies don not; hence it is criminals who usually find (and abuse) vulnerabilities. A possible solution is to change the economic analysis: provide incentives for companies and individuals to find bugs and notify the software company.⁷⁸ Several companies offer so-called bug bounty programs, which pay a fee for anyone who first

reports a bug, particularly bugs that are vulnerabilities that may lead to exploits.⁷⁹ A bounty program may also be more general and apply to bugs in software by other vendors: an

75 The Microsoft Vulnerability Research (MSVR) (<https://technet.microsoft.com/en-us/security/dn467919.aspx>).

76 See the National Vulnerability Database, which contains numerous examples of vulnerabilities of most if not all major software vendors.

77 We feel that in fact the truth is somewhere in between: further efforts may be possible, but also at some point may become prohibitively costly, while furthermore there will always be some vulnerabilities given the complications of software development at a large scale.

78 For example ENISA 2011: 123 and Barnes 2004, advocating (among other recommendations) mandatory bounty programs.

79 See generally https://en.wikipedia.org/wiki/Bug_bounty_program, referring for example to Google's Vulnerability Reward Program: <https://www.google.com/about/appsecurity/reward-program/> The Google program has been so successful that all the 'easy' bugs had been found, thereby discouraging researchers to look for deeper hidden bugs. Therefore Google has started offering Vulnerability Research Grants: <http://googleonlinesecurity.blogspot.com/2015/01/security-reward-programs-year-in-review.html>.

example is the Google project Zero.⁸⁰ Among the legal solutions discussed, which we will return to in s. 5.3.2.3 and 8.3, are imposing a stricter liability regime,⁸¹ ‘lemon laws’ for software,⁸² or a statutory obligation to follow best practices.⁸³

It should be noted that imposing higher standards on corporations that develop software commercially is not a complete solution. Software like the free Apache webserver, that is used by more than half the webserver worldwide, is open source software,⁸⁴ which means that it is provided for free and developed mostly⁸⁵ on a non-commercial basis, often by volunteers. Although it has famously been defended that open-source software is less prone to errors as ‘with enough eyes, all bugs are shallow’,⁸⁶ this has not prevented the presence of undetected exploits in open-source software. An infamous example is the Heart-Bleed bug in the OpenSSL software library.⁸⁷ The bug consisted of a simple missing bounds check, which allowed an individual to retrieve parts of the contents of RAM memory of the OpenSSL server which might contain passwords and other important data.⁸⁸ This example also shows that open source is not a panacea for preventing exploits.

Furthermore, certain vulnerabilities may be the result of configuration errors rather than a bug in the software itself. An example is a WiFi router for which the user has forgotten to change the default password, which makes it easy to hack.⁸⁹ Strictly speaking the cause of such vulnerabilities is the lack of security awareness on the side of the user. However, one might (depending on the precise circumstances) argue that the software vendor should have taken additional measures to prevent or discourage such configuration errors. Examples are forcing the user to change the default password, urging the user to use a secure default setting and allowing less secure settings only for expert users, providing configuration ‘wizards’ that guide the user through the configuration process. It may

80 See <http://googleonlinesecurity.blogspot.nl/2014/07/announcing-project-zero.html>. However, the disclosure of bugs invokes criticism by companies who claim that they have been given insufficient time to patch the bug, see <http://blogs.technet.com/b/msrc/archive/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure.aspx>.

81 Chong 2013d, also below, s. 5.3.2.3.

82 I.e. laws that allow users to return software (and be refunded) that is defective, see Barnes 2004.

83 Warner & Sloan 2012.

84 On which see Rosen 2005, Frazer 2009.

85 It is possible that a commercial company developed an improvement for open-source software that they needed for their own commercial purposes, and then made the improvement available for everyone.

86 Eric S. Raymond, in *The Cathedral and the Bazaar* (1999), available at <http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/>.

87 See www.heartbleed.com and <https://en.wikipedia.org/wiki/Heartbleed>. The bug was disclosed in April 2014.

88 There were allegations that the bug was introduced deliberately. Although in this instance there is little proof of intent, it is possible that in the future criminals will attempt to follow this path in order to create exploits.

89 This is part of the software which controls the router, hence is a software issue.

be argued that a software vendor *should* depending on the circumstances use such practices for the configuration process. Whether there is a legal obligation to do so is discussed in chapter 5.

We have up to now only discussed software vendors. Do *hardware manufacturers* also contribute to the rise of malware? The first impressions seem to be negative, in the sense that the contribution by hardware is inextricably linked to effects that we, as a society, find desirable. The connectivity and raw computing power that contributes to the spread malware are also the factors that make the Internet and its facilities so useful. No-one wants to abolish that. There are possibilities in making connectivity more secure, but these are mostly built in communication protocols that are formulated first in software. Insofar as these protocols are also hard-coded in hardware, the improvement of these protocols is not a particular issue for hardware manufacturers. We will therefore in the remainder of this report disregard hardware as such.

4.4.4. Conclusion

The main causes of security breaches are software errors (vulnerabilities) and a lack of security awareness of the user.⁹⁰ Consequentially, even perfect software cannot prevent security breaches as software cannot fully prohibit deliberate unsecure user actions, except by completely disallowing users such control over their device. However, even then a user may choose to remove these security measures by ‘jailbreaking’ the device.

Businesses that use IT are in a position to adopt secure practices, as they can obtain the expertise (by training, hiring IT employees or external IT service providers). This could lead to a reduction of security breaches. An increased diligence towards secure IT would improve security.

Software vendors may as a group, notwithstanding individual companies’ significant efforts, take more extensive action to prevent or detect vulnerabilities: increased diligence would improve general security. However, there is a lack of generally accepted effective standards and it is unclear whether the standards that have been adopted are followed in practice. Although tools to detect common vulnerabilities do exist, there is no general practice to use such tools as a matter of course. It is, furthermore, not clear whether the existing standards and tools would effectively remove or significantly reduce the vulnerabilities that lead to security breaches. The software industry is very diverse as to the programming languages and tools used and the kinds of software developed, making it unlikely that a unified approach would work across the whole spectrum of software. In addition, there

90 Cf. OECD 2008: 36 which mentions as causes of cybercrime software vulnerabilities and easy to target Internet users, besides the ease and low cost of datacommunication (the wide availability of broadband Internet).

is only limited public discussion and communication of the causes and lessons learned from specific vulnerabilities. Hence, although a greater shared sense of diligence would be beneficial, there currently exist too many hurdles to actually put such diligence into practice.

4.5. Two principal forms of cybercrime

4.5.1. Introduction

When discussing cybercrime there are two phenomena that have a central position, being both a form of cybercrime and a cause of further cybercrimes. These are *malware* and *botnets*. The central position of these forms of cybercrime merits an extended discussion, as this is crucial in understanding whether other actors may be in a position to take preventive action, either to meet a duty of care or diligence or on a voluntarily basis.

4.5.2. Malware

The root cause of many kinds of cybercrime can be found in what is called *malware*.⁹¹ Malware may be defined as “a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners” (OECD 2008: 10). Examples are spyware (malware that spies on the user), key-loggers (malware that specifically logs all keyboard input and thereby may obtain username/password combinations), ransomware (see s. 4.6.2), and botnet clients (see below).

A computer becomes infected by malware because of a vulnerability in the security

91 See extensively OECD 2008 and 2009.

of the computer, either caused by user mistakes (par 4.4.2) or software vulnerabilities (s. 4.4.3), that is exploited by a criminal. Once the malware is inserted in the computer, it can access the computer's data, software and hardware, and can monitor user actions (such as typing in passwords). The malware may further infect other computers, for example by sending out e-mails (containing the malware in an attachment) to user contacts from the e-mail program address book: contacts may be more likely to trust the attachment because it comes from a known source. The infected computer may also form part of a botnet (see s. 4.5.3). The malware often communicates with the principal criminal through the Internet: many forms of cybercrime require such communication (such as ransomware and commanding a botnet, explained in s. 4.5).

Malware is to be distinguished from computer viruses that spread from individual computer to individual computer without any further interaction with the principal criminal. Malware may also be spread deliberately from a central point, without a selfreplicating program being involved. Besides infection through Internet connections, other targeted infection methods have been known.⁹² For example, if users insert USB sticks from an unknown source in their computers, they might execute code that infects their computer with malware.⁹³

Although the consequences of malware are significant, individual users may not always be aware of the problem as many kinds of malware do not immediately or clearly affect the user. In particular botnets (see below) thrive because the user himself does not encounter any direct adverse consequences from the existence of the bot client on his computer. However, a firewall may, if correctly configured, issue a warning when unknown programs try to connect with the criminal.⁹⁴

There are strong economic incentives for developing and spreading malware.⁹⁵ The possibility of creating botnets (s. 4.5.3) provides a possibility to monetize the use of malware. It is nowadays possible to 'buy' information on unpatched vulnerabilities, as well as precoded malware that exploits known vulnerabilities and the tools to install botnet clients and control botnets.⁹⁶ The professionalization of the malware industry is indicative of the enormous size of this problem.

The relevance of malware is further increasing by the possibility that criminals will

92 Such as intentional infection by an employee.

93 Heron 2007: 13.

94 This does not work if the malware is integrated with a browser, for example by having the form of a browser extension. Cf. <http://arstechnica.com/security/2004/11/malware/6/>.

95 See OECD 2008, speaking of a malware industry. Incidentally, it has been claimed that some malware is actually spread by security services. See about the Regin malware <http://securelist.com/blog/research/68525/comparing-the-regin-module-50251-and-the-qwerty-keylogger/>.

96 OECD 2008: 32.

target the enormous market of mobile devices.⁹⁷ Admittedly, mobile devices currently have several characteristics that provide a modicum of control to prevent malware. In particular the principal requirement that applications are submitted to an official app store raises the barrier for criminals, as they will need an official front to submit the application. Once a developer is caught for submitting malware, he will probably be suspect forever unless he can explain why he did this.⁹⁸ However, the extent of the control on app stores differs. Android is relatively lenient so that it can be exploited more easily. Users can deliberately decide to bypass the app store and its controls in order to obtain more control over their device. In particular ‘jailbreaking’ opens up the device and creates opportunities for malware. Finally, a sophisticated criminal might use an exploit in the device’s operating system to install malware. A future security measure might be encrypting mobile devices.⁹⁹

In section 4.5.4 we will discuss preventive actions.

4.5.3. Botnets

A particularly relevant phenomenon connected with malware is the existence of botnets.¹⁰⁰

“A botnet is a group of malware infected computers also called “zombies” or bots that can be used remotely to carry out attacks against other computer systems”.¹⁰¹ Botnet clients have to receive their instructions from the ‘bot herder’. Wellknown communication techniques include the use of IRC (including possible backup IRC channels), P2P communi-

97 See Svajcer 2012, OECD 2008: 14, Hypponen 2006, ENISA 2011: 133.

98 For example because he was testing the process, as in the example discussed by Svajcer 2012, p. 6, referring to <http://www.eweek.com/c/a/Security/Apple-Suspends-Veteran-Researcher-from-iOS-Dev-Program-for-Exploiting-a-Bug-489867/>

99 Svajcer 2012: 9.

100 UNODC 2013: 32-35, with detailed information on international distribution of bot herders and infection, and OECD 2009.

101 OECD 2008: 22.

cation, and distributed communication between botnet clients themselves.¹⁰² The ‘ownership’ of a botnet is valuable: the botnet herder may ‘rent out’ his botnet for sending out spam or DDoS attacks.

4.5.4. *Actions against malware and botnets*

Various preventive and protective actions have been suggested to counteract the use of malware and botnets.¹⁰³ A first category of measures is preventive action to avoid infection. These have been discussed above under the headings of user security awareness (s. 4.4.2) and secure software (s. 4.4.3). Businesses may take further preventive action by proactively looking out for attempts at intrusion. They may, for example, use automated tools (including benign bots) to detect intrusions and share information that may help detect attacks and intrusions.¹⁰⁴ It has also been argued that ISPs may detect malware in Internet traffic, thereby allowing the ISP to block the intended infection.¹⁰⁵

Although individual private users may not have the skills or expertise to detect or remove malware, this is different for business users or individuals with IT expertise. Available actions are in particular: keeping anti-virus programs up to date (which would detect malware that has been discovered and signalled by the anti-virus software vendor), using a firewall (to detect malware communication or prevent such communication), regularly do a fresh re-install of the computer (which would erase most malware,¹⁰⁶ provided it does not hide in user data to reinfect the computer once certain documents are opened).

Further actions have to do with communication. The weakness of all botnets (and most malware) is that communication with the botnet herder is necessary. By cutting off the communication channel used, the botnet client is rendered harmless. Furthermore, the communication may reveal the presence of the botnet. However, botnets may employ a variety of methods to complicate this, such as having multiple alternatives for communication or hiding between legitimate Internet communication. An ISP can only look for botnet communication if it knows how to distinguish this from legitimate communication.

A business user may have more resources at his disposal.¹⁰⁷ For example, regular security audits¹⁰⁸ may track infections and may show weaknesses in the system configuration and security strategy. If a computer owned by a business is suspected of being

¹⁰² Heron 2007, OECD 2008: 24-25.

¹⁰³ Extensively ENISA 2011.

¹⁰⁴ Gold 2009.

¹⁰⁵ http://www.lavasoft.com/support/spywareeducationcenter/wp_ispmalwarefiltering.php.

¹⁰⁶ Except if the malware would have installed itself in the computer firmware, which is not erased with a fresh re-installation of the software.

¹⁰⁷ Also Pinguelo, Lee & Muller 2012: 82-85.

¹⁰⁸ Mueller 2006.

infected, an IT professional could monitor all network traffic closely.¹⁰⁹ If the computer is not used for other purposes, all Internet traffic automatically becomes suspect. It is noteworthy that IT professionals have been able to track botnet herders.¹¹⁰ ISPs may also place themselves in a position to monitor a malware-infected computer, for example by deliberately leaving a computer unprotected in order to trace any malware installed on it.¹¹¹ A more general measure for detecting malware communication is the use of firewalls, which may signal suspicious attempts at communication.

Botnet clients in particular may be detected by particularities in their network behaviour. If, for example, large amounts of spam are sent out by a botnet, the ISP of (part of) the botnet clients may become aware of the spam and determine which of the ISP's customers are apparently infected.¹¹² The ISP may warn the customer or even block the customer from Internet access,¹¹³ thereby providing a strong incentive for the customer to clean his computer and increase his security efforts.¹¹⁴ In section 7.4 we will return to the question whether they are actually legally allowed to monitor traffic and block users: here we only stipulate that technically they may be able to. Incidentally, an ISP may also at the receiving end filter for and block spam, thereby limiting the possibility of infection by spam e-mail.

Blacklisting is a technique whereby non-profit and commercial organisations may contribute to combating botnets, spam and the distribution of malware.¹¹⁵ It consists of an organisation keeping a list of 'suspect' IP addresses and/or domains. Subscribers to the particular blacklist can then refuse to allow traffic to and from the blacklisted addresses. A similar method is employed by several large search engines, including Google,¹¹⁶ which flag suspect websites by pointing out that the website appears to contain malware (either deliberately placed by the website owner, or placed by a third party who illegally obtained access to the server). Several web browsers also have declared to incorporate warnings for suspect websites.¹¹⁷ Related to blacklisting, ISPs may be able to, or even requested to, prohi-

¹⁰⁹ Mueller 2006 speaks of 'perimeter monitoring', and points out that this is inefficient given the vast amount of innocent traffic that has to be filtered out. Such monitoring is done using a so-called packet sniffer, network analyzer, or comparable tool.

¹¹⁰ See for example <http://www.theverge.com/2012/3/26/2902786/microsoft-zeus-botnet-raid-pennsylvania-illinois>. It is not entirely clear in which way the botnet herder was identified.

¹¹¹ Such a computer is called a malware 'honey pot'.

¹¹² Van Eeten a.o. 2010 provide an empirical analysis showing large differences between infection rates of legitimate ISPs, suggesting that some have more effective practices than others.

¹¹³ Extensive suggestions can be found in OECD 2012b, also ENISA 2011: 122-123, 127-128. The ISP would only allow connection to pages with information on the malware and instructions on how to remove it.

¹¹⁴ As argued by OECD 2008: 29, Barnes 2004: 329.

¹¹⁵ OECD 2009: 35-37.

¹¹⁶ See the Google warning "This site may harm your computer.",

¹¹⁷ See for example Firefox, <https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work>, or Chrome, <https://support.google.com/chrome/answer/99020?hl=en>.

bit access to known malware distribution websites.

In particular cases software vendors may also be in a position to help combat malware and botnets. An example is Microsoft, which in the course of detecting counterfeit copies of its operating system may also find infections by malware.¹¹⁸ Operating system software vendors may be in a particularly strong position to detect some kinds of malware, as they may have massive amounts of data on reported user problems, part of which concerns problems with malware infection.

It follows that businesses, ISPs and software vendors have various actions open to help to prevent and combat malware and botnets.

4.6. Two specific forms of cybercrime

4.6.1. Introduction

The use of malware and botnets is, in itself, criminal, being a breach of computer integrity. It may also provide the starting point for further crimes. Two specific forms are discussed here: ransomware (which is a special case of malware) and DDoS attacks (which are a particular use of botnets).

4.6.2. Ransomware

Ransomware may be described as malware that “attempts to extort money from a victim by encrypting files and demanding payment for their restoration.”¹¹⁹ The victim usually receives a message, most frequently on his computer, that demands him to pay a sum of money or perform some other action in order to receive a password that will allow him to access his files again.¹²⁰ Ransomware has been found as early as 1989.¹²¹ Criminal enforcement against the use of ransomware often proves difficult as it does not clearly fall under the remit of one specific authority.¹²²

Theoretically, ransomware might also operate by threatening to publicise files that the victim would prefer to keep private, such as compromising pictures or confidential data,¹²³ or alternatively by using the data found for malicious purposes (such as identity theft or

¹¹⁸ <http://www.theverge.com/2012/9/13/3325516/microsoft-nitol-botnet-after-discovering-pcs-sold-to>.

See also for a different case (where again the detection method used is not clear) <http://www.theverge.com/microsoft/2012/1/24/2729742/kelihos-botnet-ex-antivirus-worker>.

¹¹⁹ Bridges 2008. OECD 2008: 16-17 identifies ransomware as one example of malware.

¹²⁰ See Luo & Liao 2007 for a detailed analysis of several ransom methodologies.

¹²¹ Bridges 2008: 18, referring to information on the PC Cyborg (AIDS) Trojan Horse at <http://www.ciac.org/ciac/bulletins/a-10.shtml>.

¹²² Bridges 2008: 19, referring to a case where the local police decided it was an international Internet crime.

¹²³ The infamous Sony hack of 2014, alleged initiated by the North Korean government, is an example of this. Embarrassing internal e-mails were found and made publicly available.

using accounts for ordering goods and services). However, such approaches are usually not considered to fall under ransomware, properly speaking, in the relevant body of literature. We will therefore not consider this possibility any further.

A schematic representation of the relevant actors and the causal relations between their areas of influence can be given as follows. This figure is similar to the figure for malware in general, as ransomware is simply a species of malware.

The consumer owns a computing device, such as a computer or smart phone, which becomes infected. The infection allows the criminal to lock away (encrypt) valuable data, and threaten to destroy it.

Ransomware is the result of an infection, the causes of which have been described in section 4.4. General preventive actions against malware have been described in section 4.5.4. These also apply to ransomware, and include raising user security awareness,¹²⁴ and tools like pop-up blockers (as infection often occurs through pop-ups that are clicked on).¹²⁵ Furthermore, anti-virus programs could help to detect and eliminate ransomware before it becomes active.

The infection and subsequent communication by the criminal to the consumer usually occur through the Internet, which allows for practically untraceable communication by the criminal as well as relatively secure and anonymous payment facilities. A sufficiently strictly configured firewall might be able to block the communication, dependent on the kind of communication and any alternative channels programmed in the ransomware. Theoretically

¹²⁴ Luo & Liao 2007.

¹²⁵ Luo & Liao 2007: 201.

ISPs could help in tracing ransomware communication if they are informed about instances of ransomware infection and the communication with the criminal at a specific time, but in practice there do not appear to be significant notifications. Moreover, ISPs are not under a general obligation to help trace the criminal behind the ransomware.

There are also specific precautions to take against a future ransomware infection. The only failsafe defence against ransomware is making regular backups.¹²⁶ These should ensure the accessibility of the unencrypted files on an earlier backup. Automated tools for backups help the user to backup regularly; these may use local backups on a hard disk or backups 'in the cloud' (at a dedicated server such as Dropbox). Antivirus programs also function as a preventive measure, but they only detect known threats. Until recently, experts managed on occasion to decrypt the encrypted files, but it is generally expected that ransomware creators will turn to even more advanced cryptographic techniques that will be practically proof to decryption.¹²⁷ Once ransomware has encrypted data, the only option besides paying appears to be to determine the decryption key, which may be unfeasible if a sufficiently strong encryption key is used.¹²⁸

With respect to the tracking of the ransom payments, there may be various options to do so, but these would generally require the aid of law enforcement.¹²⁹

To conclude: additional actions against ransomware (besides those applying to malware in general) are:

- regular backups by the user,
- finding the decryption key (which requires highly specialised expertise).

4.6.3. DDoS attacks

Distributed Denial of Service (DDoS) attacks are concentrated attacks on a website server or groups of server that are designed to render the website unavailable (which leads to a Denial of Service).¹³⁰ The attack creates an artificial congestion of the server by sending large amounts of communication requests. The difference between a general 'denial-of-service' attack, which can be executed by a group of human users, and a DDoS attack is that the latter is performed automatically by a distributed group of computers controlled by one person, typically carried out through botnets.¹³¹ In practice several users may combine to operate several botnets: these are also called DDoS-attacks. We will hereafter focus solely

¹²⁶ Bridges 2008: 20. However, a sophisticated criminal might try to use the ransomware to also delete the backups when the backup devices are attached to the computer in order to make new backups.

¹²⁷ Luo & Liao 2007: 199, Bridges 2008.

¹²⁸ Oswald 2006.

¹²⁹ See also MacCarthy 2010, and Mann & Belzley 2005, who suggest a role for payment providers.

¹³⁰ Cf. Sinrod & Reilly 2000: 189ff, Pinkney 2002: 590, McLaurin 2011, Chandler 2004.

¹³¹ OECD 2008: 15 lists DDoS attacks as one goal of malware in the form of botnets.

on DDoS-attacks operated with botnets. The damage caused by a DDoS-attack can be significant.¹³²

It should be pointed out that it may be more or less easy to find the actual principals of the attack, depending on the specifics of the attack. An example is a DDoS attack on PayPal that was committed with a tool that sent the IP-address of the user of the tool, thereby making it easy to trace the originator.¹³³

It has been argued that DDoS-attacks are not inherently wrong, as they may be the online equivalent of offline protests or public demonstrations.¹³⁴ However, it is nowadays widely accepted that DDoS-attacks are not a legitimate form of protest.¹³⁵

As we presume that the DDoS attack is performed with botnets, the general preventive actions are the actions which can be taken against malware and botnets (s. 4.5.4). There are also some additional measures which businesses and their ISPs can take to strengthen the IT infrastructure against a DDoS attack.¹³⁶ The infrastructure may be made more robust in order to avoid interdependencies between different services. Once the DDoS attack starts, a number of emergency measures are available, such as switching to backup servers and filtering user requests.¹³⁷ ISPs might help to trace the sources of the attack, in particular the computers (at least, the IP-addresses) that send the requests.

¹³² Kaspersky Lab 2015 mentions \$ 52.000 for small-to-medium-sized businesses and \$ 444.000 for larger enterprises, besides reputational damage.

¹³³ <http://www.darkreading.com/attacks-and-breaches/anonymous-ddos-attackers-in-britain-sentenced/d-d-id/1108360?>

¹³⁴ Evgeny Morozov, 'Parsing the impact of Anonymous', available at http://neteffect.foreignpolicy.com/posts/2010/12/09/parsing_the_impact_of_anonymous. Critically McLaurin 2011: 232-246.

¹³⁵ See the legal position in the jurisdictions described in chapter 5, and OECD 2008: 15.

¹³⁶ These are rather technical. See for a somewhat more accessible discussion in Dutch: Jacobs 2013.

¹³⁷ For example with the aid of CAPTCHAs (a requirement that a user has to recognise characters in a deliberately obscured picture, which supposedly would only be possible with human intervention).

These computers might – if permitted by applicable legal rules and the ISP contract – be (temporarily) cut off from Internet connectivity, or at least prevented from sending request to the server under attack. Additionally, selective blocking of traffic (to the server under attack) from ISPs from where many requests originate might help. Furthermore, ISPs might be able, by combining patterns in communication, to trace the botnet herder behind the attack. A business might also hire specialised forensic services to help find the origin of the attack.

4.7. Actors and actions

The full picture of the most important and relevant causes, contributing factors, and possible preventive actions as discussed above can be graphically represented as follows (with some simplifications).

If we focus on the actors involved in the occurrence of cybercrime, this is the result.¹³⁸

- ISPs: detect malicious activity, detect and trace malware communication; detect network patterns of botnets; blacklist websites; filter spam; warn users that have been infected by malware; block users that have been infected by malware; blacklist originators of DDoS attack requests; provide aid to law enforcement and private forensic investigations.

¹³⁸ See also the list of proactive prevention strategies in OECD 2008: 52, and the analysis of Barnes 2004 and Chandler 2004 of contributing factors.

Furthermore an ISP may quickly implement new Internet standards and best practices instead of lagging behind.

- software vendors: develop better quality software, implement better development standards and secure development attitudes; encourage and organise detection of vulnerabilities; on occasion help with malware detection and investigation.
- businesses: regularly update software; increase security awareness and practices; use a virus scanner; install firewall; monitor for suspicious network traffic; make regular back-ups; have alternatives to IT services/websites; forensic investigation.

It should be noted that this only lists possibilities. Assumedly many companies actually already take many of these actions, or conversely there may be reasons why some of these actions are found undesirable.

There are other actors that may take preventive measures. In particular search engines and browsers can (and regularly do) take steps to detect malicious activity or block black-listed websites. Additionally, a variety of other actors may contribute to further prevention. Domain name registrars may also play a part in the prevention of distribution of malware, by being more proactive towards domain names that are used primarily for distribution of malware.¹³⁹ Payment providers may track or block pay-ments.¹⁴⁰ WiFi providers could disallow anonymous connections or alternatively could trace activity.¹⁴¹ However, these actors are not as influential as the three groups identified above. Examination of their role is to be left for future research.¹⁴²

Incidentally, it has also been claimed that state actors are responsible for some forms of cybercrime or cyberattacks.¹⁴³ If this is true, this could lead to mixed signals towards cybersecurity from the governments involved: completely secure systems would, for example, make cyberespionage more difficult. As the role of governments as such is not part of the scope of this report, we will not discuss this issue further.

Finally, Internet architects, parties responsible for the design of the Internet infrastructure, could take into account the aim of cybercrime prevention.¹⁴⁴ We will discuss this briefly in section 6.6.3.

¹³⁹ See OECD 2008: 52: “The possibility to include security and abuse management in registrar accreditation procedures and contracts.”, also OECD 2009: 122-129.

¹⁴⁰ Mann & Belzley 2005.

¹⁴¹ Cf. Watkins 2013 on the role of WiFi providers.

¹⁴² This is in line with other reports that suggest focusing on key business players or sectors, for example OECD 2012a: 44.

¹⁴³ Cf. NCSC 2014: 69-71.

¹⁴⁴ See s. 6.6.3, also Brenner & Clarke 2005: 28.

4.8. Conclusion

The three topics at the center of this research are security of hardware and software, ransomware, and DDoS attacks. Our preliminary investigation in the actors and causes involved points to three principal contributory actors, next to the possible victims of cybercrime. The focus will be on:

- Internet Service Providers
- software vendors

businesses as being the victim of cybercrime.

The actions that these actors can take are primarily:

- ISPs: various actions, which might all be encompassed by a general duty of care and diligence.
- software vendors: more efforts towards creating more secure software, which can be interpreted as a duty of diligence towards the development of software.
- businesses: back-up and fall-back scenarios against DDoS attacks; improved security practices. These can be considered part of general duties of care and diligence towards their customers.

A number of other actors have the possibility to take actions that could contribute to a decrease in cybercrime, but those actors are *prima facie* not under a legal obligation to take such actions. These actors will only be discussed incidentally, in particular when alternative compliance measures are discussed (s. 8).

5. Duties of care and diligence regarding three topics of cybercrime

5.1. Introduction

At present, most jurisdictions have provisions that criminalize the primary acts of cybercrime. Less clear is the law as regards persons or institutions that could prevent cybercrime. In the following document, we examine to what extent the actions that can be taken to prevent or discourage cybercrime in the three forms or topics that we discussed are legally obligatory. We will analyse the law in the four jurisdictions selected for this report. The focus will be on private law, where obligations and duties of the principles actors – ISPs, software vendors, and businesses – will be discussed in the general framework. Furthermore criminal law and administrative law will be discussed insofar as relevant.

5.2. The Netherlands

5.2.1. Introduction

The Netherlands is a civil law jurisdiction. The legislator regularly updates statute law to keep abreast of new developments. Next to statutory law, case law is recognised as an important source of law.

5.2.2. Private law

The Dutch civil code was originally heavily influenced by the French Code Civil, but it was recently recodified on the basis of extensive comparative research. As a result, the new Dutch Civil Code (*Burgerlijk Wetboek*, hereafter BW) was introduced in 1992.

5.2.2.1. General contract and tort law

As regards private law obligations to care it is necessary to examine both the general framework in which specific obligations are determined, as well as the specific relations that may exist between parties, as these influence the existence and extent of obligations.

In Dutch contract law in general, the obligations of parties follow from the contractual agreement, both explicitly and implicitly.¹⁴⁵ The interpretation of contracts looks at both the text and other contextual clues,¹⁴⁶ while default law and mandatory law provide additional rules and obligations. Specific kinds of contracts are subject to specific rules and obligations, for example rules concerning contracts for sale or service contracts. Additionally,

¹⁴⁵ Hartkamp & Sieburgh 2014: nr. 354-390.

¹⁴⁶ See the leading cases HR 13 March 1981, NJ 1981/635 (*Ermes/Haviltex*) and HR 20 February 2004, NJ 2005/493 (*DSM /Fox*).

the concrete circumstances of the case may give rise to specific obligations on the basis of general fairness (*redelijkheid en billijkheid*, art. 6:2 and 6:248 BW).¹⁴⁷ This is an important source of judge-made rules.

Liability for breach of contract (*niet-nakoming*) requires attributability (*toerekenbaarheid*, see art. 6:75 BW), which, however, is generally presumed. The debtor has to prove that the breach is not attributable to him.¹⁴⁸ However, this leaves open the prior question whether there is a breach of contract.¹⁴⁹ The mere fact that a result desired by the creditor is not reached does not necessarily imply breach: only if this result was actually contracted for as a matter of obligation, will a failure to achieve it constitute breach. Dutch law follows the French doctrinal construct of obligations of result versus obligations of means.¹⁵⁰ In case of an obligation of result, the fact that the result was not reached leads to liability unless the debtor proves that the breach was due to *force majeure* (*overmacht*), i.e. that the primary cause of the default is not attributable to him. In case of an obligations of means, the debtor is only required to give his best effort, provide the care of a good service provider (art. 7:401 BW), or act like a reasonably knowledgeable and reasonably acting professional,¹⁵¹ as the norm may be for the situation at hand. The debtor has to provide appropriate care for all contracts, a norm for which the specific circumstances, including the kind of contract, may lead to more detailed rules. This also applies to contracts for specific results if the stipulation to achieve these results gives rise to additional obligations to protect or promote the result, as it generally does. The civil code contains provisions for such obligations to care for a number of specific situations, but they are generally assumed on the basis of the general duty of fairness (art. 6:248 lid 1 BW).

For tort law in general the main article is 6:162 BW, which provides the liability of persons for unlawful acts (*onrechtmatige daad*). The law provides three categories of unlawful acts. An unlawful act can consist of an infringement of a right, a violation of statutory duty, or an act which is contrary to unwritten law according to the demands of social conduct. An omission may also constitute an act in the sense of art. 6:162 BW. In practice the third category, acts which are contrary to unwritten law,¹⁵² is the most important one as it provides courts with wide discretion to adapt the law to changing circumstances. In this respect it fulfils a function similar to the tort of negligence in common law systems. It is noteworthy

¹⁴⁷ For example in HR 19 October 2007, NJ 2007/565 (ETC/Vodafone).

¹⁴⁸ Cf. Hartkamp & Sieburgh 2012: nr. 370.

¹⁴⁹ See for the following Hartkamp & Sieburgh 2012: nr. 332-362, De Jong 2006, Tjong Tjin Tai 2004a and 2004b.

¹⁵⁰ See generally Den Tonkelaar 1982, also HR 14 April 2006, NJ 2006/259.

¹⁵¹ HR 9 November 1990, NJ 1991/26 (Speeckaert/Gradener).

¹⁵² Under the old civil code this was called the '*zorgvuldigheidsnorm*', the norm to act according to the demands of diligence. Nowadays it is more usual to speak of '*zorgplichten*'.

hy that Dutch courts are more likely to find a duty to prevent harm to third parties than judges in common law systems. An example is liability for leaving your car running, thereby allowing a joyrider to take your car and causing damage.¹⁵³ Liability for pure omissions is also possible, although case law requires that there has to be at least consciousness of the risk or some specific connection to the harm.¹⁵⁴ This is understandable: because one cannot care for the whole world, some specific antecedent connection or at least close proximity to the harm is required for there to be duty of care to act against a harm one has not caused oneself.

Besides personal liability, Dutch law recognises the usual kinds of vicarious liability and risk-based forms of liability (for animals etcetera). There are, furthermore, a number of specific articles for specific kinds of liability. Product liability is recognised in art. 6:185 BW. However, this is only applicable to tangible, movable objects ('roerende zaak', see art. 6:187(1) BW).¹⁵⁵

In this regard, art. 6:196C BW is of special importance. This provision is an implementation of arts. 12-15 E-commerce Directive 2000/31/EG. These articles provide an exemption from liability for Internet Service Providers (ISPs) who only operate passively as regards the Internet traffic or content. See further sections 5.2.2.2 and 7.4. As a result of the Directive, the legal obligations of many ISPs regarding the content they make available or transmit are limited.

5.2.2.2. *Software vendors*

Software vendors may be held liable for bugs that cause vulnerabilities in their product insofar as these bugs are not to be expected or hinder the agreed-on usage of the product. The norm in case of a contract of sale (which applies in principle to the sale of software)¹⁵⁶ is that the product should possess the characteristics which the buyer could legitimately expect on the basis of the contract, taking into account among others the nature of the product and the information provided by the seller. In particular, the buyer may expect that the product has the characteristics necessary for normal use of the product and of which he

¹⁵³ HR 2 December 1966, NJ 1967/42 (Haringkar).

¹⁵⁴ Particularly the leading precedent HR 22 November 1974, NJ 1975/149 (Struikelende broodbezorger). Generally: Smits 2000, Giesen 2004, Tjong Tjin Tai 2007b.

¹⁵⁵ Dommering-Van Rongen 2000, Westerdijk 1995.

¹⁵⁶ See HR 27 April 2012, ECLI:NL:HR:2012:BV1301, NJ 2012/293 (Beeldbrigade) for standard software. The Hoge Raad ruled that it is not relevant whether the software was provided on a tangible carrier, or provided online. In case of tailor-made software it is likely that the rules for service contracts are applicable.

had no reason to doubt the presence.¹⁵⁷ When applied to bugs that may facilitate infection with malware, this criterion does not appear to cover vulnerabilities, as these often do not hinder the normal use of the software: they only lead to undesirable side effects. Furthermore, sellers generally take care not to promise a completely secure, bug-free product: when general information and advertisements appear to promise security, the detailed terms and conditions often negate this promise.¹⁵⁸ On the other hand, at present software is arguably expected to at least try to avoid vulnerabilities that leave the computer open to intrusions and malware infections. It seems unlikely that software vendors will openly announce that their products do not follow any standard of security. The provisional conclusion is that software will be held to some standard of security, which leads the vendor to have a contractual obligation to avoid vulnerabilities.¹⁵⁹ This obligation does not amount to a guarantee that the software is bug-free.

The fact that software may be provided for free does not in itself preclude liability.¹⁶⁰ Although this situation does not amount to a contract of sale, general contract law may lead to liability, approximately following the same standards as with the contract of sale. Liability may, however, be limited due to the conditions under which the software was provided¹⁶¹ (usually a license agreement disclaiming all warranties, in particular not guaranteeing the absence of defects¹⁶²). There are, however, indications in case law that liability may still exist if the warnings were insufficiently precise to indicate the exact kind of danger.¹⁶³

The obligation to avoid vulnerabilities is rather weak: it is akin to a duty to take care to avoid vulnerabilities. If there is no guarantee that the software is bug-free, the logical consequence is that the software is permitted to contain bugs. It is practically impossible

157 See art. 7:17(2) BW as applied to a software product. The literal text is: “Een zaak beantwoordt niet aan de overeenkomst indien zij, mede gelet op de aard van de zaak en de mededelingen die de verkoper over de zaak heeft gedaan, niet de eigenschappen bezit die de koper op grond van de overeenkomst mocht verwachten. De koper mag verwachten dat de zaak de eigenschappen bezit die voor een normaal gebruik daarvan nodig zijn en waarvan hij de aanwezigheid niet behoefde te betwijfelen, alsmede de eigenschappen die nodig zijn voor een bijzonder gebruik dat bij de overeenkomst is voorzien.”

158 The terms and conditions are relevant for determining the precise content of the contract, cf. HR 5 June 2009, NJ 2012/182-184 (Effectenlease).

159 Cf. the somewhat inconclusive discussion in Girot 2001: 153-160.

160 See for example regarding the possibility of liability for gratuitously provided information (albeit this concerned the government) HR 25 May 2012, NJ 2012/340 and third party liability for free legal advice HR 4 October 1996, NJ 1997/594.

161 This applies even in the case of strict liability, where an agreement may on the basis of contributory negligence lead to a partial or full reduction of damages, cf. HR 25 October 2002, NJ 2004/556 (Paardrijles). This amounts to what is elsewhere called assumption of risk.

162 Blok 2010: 111-112.

163 HR 27 May 1988, NJ 1989/29 (Veenbroei), HR 28 May 2004, NJ 2005/105 (Jetblast), also HR 25 November 2005, NJ 2009/103. Admittedly these cases involve physical damage to persons.

to quantify the amount of bugs, or set quality standards as to the kind of bugs that the software might or might not contain. It would, though, be possible to provide statements as to methods, best practices, checks and processes that were used in developing the software.¹⁶⁴ It is possible that standards are developed which lead to a reduction of certain kinds of bugs, for example an automated check on buffer overload. Such rules might then be used to specify the concrete contractual obligations. Presently this is uncommon, and there is no evidence of a customary rule to this effect that might have legally binding force.

Besides the obligation to avoid vulnerabilities, the software supplier may be under an obligation to repair known vulnerabilities in due time. It is not entirely clear whether this is a legal obligation or rather a reaction to market pressure. If software is not 'patched' soon enough, security companies often advise clients to stop using the vulnerable software.¹⁶⁵ Evidence that patches and updates are not considered a legal obligation may be found in the fact that software may become obsolete, reach the end of life, or be discontinued: the supplier announces that he will no longer update the software or repair any new vulnerabilities found. This may be either construed as a limitation to any contractual obligation to update, or as evidence that there is no obligation to patch at all (in which case the announcement simply means that the supplier does not care if the product would no longer be used).

Insofar as there is a legal obligation to repair known vulnerabilities, this amounts to an obligation to provide a patch within reasonable time. It is impossible to provide a patch immediately after being notified of the vulnerability: patching takes time (because of the necessity of analysis, programming, testing). In the meantime the vulnerability remains open to exploitation. The only option open to the user is to avoid the product. Once the patch is available, it is up to the user to install it (although it is increasingly common to have automated update mechanisms). If the user neglects to do so, any claim against the supplier would probably fail due to contributory negligence on the user's part.

Finally, as regards a secure configuration process (see s. 4.4.3, end), there is not even discussion as to whether it is legally required to follow a secure configuration process. On the one hand, many software vendors do follow such practices, which are continually improved with the experience that comes from earlier security breaches. On the other hand, to qualify the lack of a secure configuration process as a breach of contract appears to over-extend the law. Contracts usually do not contain any clauses on the configuration process, while it cannot be said at present that secure configuration processes are so essential to the

¹⁶⁴ Such standards may be set by standards organisations like ISO.

¹⁶⁵ This has even happened to major software of major companies, such as Microsoft's Internet explorer. See for example <http://www.reuters.com/article/2014/04/28/us-cybersecurity-microsoft-browser-idUSBREA3QoPB20140428>.

software that the contract can be assumed to include an implicit, mandatory guarantee to that effect.

As the analysis shows, there is presently not much ground for liability on the part of the software vendor liable. Even if there would be breach of contract, this will usually not lead to an award of damages, because of the prevalence of exemption clauses in software contracts and licenses.¹⁶⁶ Exemption clauses are generally allowed and upheld under Dutch law, except insofar as the clause exempts liability for an intentional breach of contract caused by the directors of the company.¹⁶⁷ Courts may find reason to set aside an exemption clause also in specific circumstances. An example is a case in which a non-profit organisation had hired a computer company to automate its operation.¹⁶⁸ Given the way in which the exemption clause had become part of the contract, the relation between parties, in particular the dependence of the organisation of the expertise of the computer company, the interest involved with the agreed upon work, and the seriousness of the breach, the exemption clause was set aside as it was found to be unfair.

Third-party liability of software suppliers towards non-clients is usually not considered. This suggests a broad consensus that there is insufficient ground for third-party liability. A claim by a non-contracting party against a software supplier would have to be based on negligence as violation of unwritten law (*schending van de zorgvuldigheidsnorm*), art. 6:162 BW. In an example scenario, a company suffers from a DDoS attack, which is caused by a botnet that came into being partly by the existence of a vulnerability that led to many malware infections. As this example immediately makes clear, any claim on the basis of negligence would run into practically insurmountable difficulties as to proof of causality (did the specific vulnerability lead to the botnet?), the existence of many other contributing factors, the remoteness of the damage, and the possibility that the company's interests are outside of the scope of protection of the norm ('relativiteit'). It seems unlikely that it is found unlawful towards third parties to leave vulnerabilities in software, and in any case a claim on the supplier is almost certain to fail due to other difficulties.

Although it has been defended that the rules of product liability should apply to software under certain conditions,¹⁶⁹ at present this is not recognised. Hence this is not a relevant ground for liability.

¹⁶⁶ Blok 2010: 112-113, more general 82-89, also De Graaf & Schuurman 2014: 79.

¹⁶⁷ Wessels, Jongeneel & Hendrikse 2010, § 14.6.2 and 14.7, Hartkamp & Sieburgh 2012, nr. 364-369.

¹⁶⁸ Gerechtshof Amsterdam 22 November 2001, LJN AD7868, Computerrecht 2002/2, p. 94 (Kirche in Not/Cap Gemini).

¹⁶⁹ Westerdijk 1995, arguing for this if the software is delivered on a tangible carrier.

5.2.2.3 Internet Service Providers

Regarding Internet Service Providers, the law stands as follows:¹⁷⁰ In order to implement arts. 12-15 E-commerce Directive 2000/31/EC, the Dutch legislator has added art. 6:196C BW. This article contains an exemption of tort liability for Internet Service Providers on the condition that they have not actively been involved with the information they store or transmit. Art. 6:196C BW and arts. 12-15 E-commerce Directive specifically mention the activities of hosting, ‘mere conduit’ (only transmitting data), and temporary storage (in particular caching). The ECJ has explained these requirements as follows: the exemption applies if the ISP has not played an active role of a kind which gives it knowledge of, or control over, the data stored.¹⁷¹ The ECJ refers to recital 42 in the preamble to the E-commerce Directive, according to which the exemptions from liability only cover cases in which the activity of the ISP is ‘of a mere technical, automatic and passive nature’.¹⁷² The exemptions apply irrespective of whether the service is provided for remuneration or for free.¹⁷³ Search engines can also fall under these exemptions: they are service providers in the meaning of the E-commerce Directive.¹⁷⁴

Regarding the lack of knowledge required for the exemption, art. 15(1) E-commerce Directive specifically stipulates that member states shall not impose a general obligation on ISPs “to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.”¹⁷⁵ Hence knowledge of the illegal activity is mostly derived from an actual complaint by a third party, which may require the ISP to remove the information or block access to it.¹⁷⁶ Furthermore, it is possible that the knowledge of the ISP derives from “an investigation undertaken on its own initiative”.¹⁷⁷

However, it does not follow that ISPs are not subject to any obligations whatsoever. Art. 15(2) E-commerce Directive allows member states to establish obligations for ISPs “promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service”, as well as obligations to cooperate with the authorities by helping with identification of hosting clients.

170 Generally: Schellekens 2001, Van Eijck 2010, Den Dekker & Van der Linden-Smith 2014, also Van der Net 2000.

171 ECJ 23 March 2010, cases C-236/08-C-238/08 (Google Adwords), nr. 120.

172 ECJ 23 March 2010, cases C-236/08-C-238/08 (Google Adwords), nr. 113.

173 ECJ 23 March 2010, cases C-236/08-C-238/08 (Google Adwords), nr. 116.

174 Cf. ECJ 23 March 2010, cases C-236/08-C-238/08 (Google Adwords).

175 Confirmed in ECJ 12 July 2011, C-324/09 (L'Oréal/eBay), nr. 139.

176 Cf. the American practice of Notice and Take Down.

177 ECJ 12 July 2011, C-324/09 (L'Oréal/eBay), nr. 122.

If the ISP does not meet the requirements for the exemption of liability, it is not necessarily liable. In this case the national court will have to determine whether the ISP is liable following the national tort law.¹⁷⁸

As the case law of the ECJ is binding as regards the interpretation of these articles, it also determines the state of Dutch law. As a result, an ISP that is completely neutral and passive as to the data transmitted or stored cannot be held liable. If the ISP is informed of illegal activity, he may no longer be exempt from liability, depending on the circumstances of the case.¹⁷⁹ Paradoxically, if the ISP takes initiative to detect illegal activity, that may make him more likely to be liable as he becomes more knowledgeable of the activities conducted through his service. The ISP may be liable insofar as he has been informed of illegal activity of a client and still refuses to act, even though the notice is clearly well-founded.

These rules do not, however, preclude specific obligations to block illegal activity. A sufficiently clearly specified judicial order to block for example commands from a botnet herder (identified by IP or in another way) might be allowed. The ECJ only prohibits a general monitoring duty that is disproportionate or excessively costly.¹⁸⁰ Furthermore, an ISP may be required to cooperate to find the identity of clients who may conduct illegal activity if this is in accordance with national law.¹⁸¹ EU law does not require national law to impose such an obligation.¹⁸² In the Netherlands, such an obligation does exist,¹⁸³ although whether the court actually imposes an order depends on the circumstances of the case.¹⁸⁴

As regards the contractual liability of the ISP towards clients who have become victim of malware, ransomware, or DDoS attacks, the following applies.¹⁸⁵ An ISP generally operates on the basis of a service contract,¹⁸⁶ so he is held to the care of a good service provider (art. 7:401 BW). He is thereby required to undertake actions to protect or promote

¹⁷⁸ ECJ 12 July 2011, C-324/09 (L'Oréal/eBay), nr. 108.

¹⁷⁹ It is to the national court to look at the specific circumstances in order to determine whether the notice was sufficient (combined with possible investigations by the ISP himself) to amount to the 'knowledge' that is required to block an appeal to the exemption. See ECJ 12 July 2011, C-324/09 (L'Oréal/eBay), nr. 122, which appears to require a sufficiently precise and adequately substantiated notification.

¹⁸⁰ ECJ 12 July 2011, C-324/09 (L'Oréal/eBay), nr. 139: "the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website. Furthermore, a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly." See further ECJ 24 November 2011, case C-70/10 (Scarlet Ex-tended/Sabam) and ECJ 16 February 2012, case C-360/10 (SABAM/Netlog).

¹⁸¹ ECJ 12 July 2011, C-324/09 (L'Oréal/eBay), nr. 141-142, cf. art. 15(2) E-commerce Directive

¹⁸² ECJ 29 January 2008, case C-275/06 (Promusicae/Telefónica).

¹⁸³ HR 25 November 2005, NJ 2009/550 (Lycos/Pessers).

¹⁸⁴ See case law in *Groene Serie Onrechtmatige Daad*, art. 196C (Scheltema & Tjong Tjin Tai), comment 14.

¹⁸⁵ Extensively Siemerink 2007.

¹⁸⁶ Siemerink 2007: 88-94.

the relevant contractual interests of the client, which may be further specified or limited in the contract. Although an ISP could provide only a barebones facility, ISPs often offer additional services such as offering virus scanner, spam filters, filtering for undesirable content.¹⁸⁷ Generally, ISPs contractually stipulate that their services only oblige them to endeavour to the care of a good service provider, which is an obligation of means.¹⁸⁸ This would apply to most additional services provided by the ISP, although on occasion the contract might contain specific quality requirements amounting to an obligation of result.¹⁸⁹ An ISP would have to take some measures against malware, but cannot offer complete security.¹⁹⁰

Regarding liability: ISPs generally stipulate in their contracts exemptions from any obligation to pay damages. These exemptions will generally be valid.¹⁹¹

As a consequence, users will generally have no recourse to ISPs if they have been infected by malware, except if the ISP can be proven to have neglected to take the required safety measures and the exemption clause is, moreover, found to be invalid in the specific case, which would in general require gross negligence from the directors of the ISP.

The corporate clients of an ISP may be in a better position to negotiate more friendly terms. A corporate contract regularly includes terms and conditions on the 'uptime' of communication/Internet connectivity and on possible security measures. The ISP may even assume a more extensive role as IT advisor, thereby taking over part or whole of the IT services of the client (outsourcing). In such a case, the ISP will be subject to more extensive obligations to care by taking preventive measures, such as the detection of malware and illegal activity or the provision of backup equipment and software in case of attacks. This leads to a real possibility that the ISP may be found to be in breach of contract. Corporate contracts still often contain exemption clauses, but these tend to be less restrictive than the clauses in consumer contracts, as a result of which the ISP theoretically could be required to pay significant damages. However, the amount of compensation that would be awarded is in practice usually much lower than the limits in exemption clauses. First of all, pure economic loss is frequently excluded, and this type of loss is usually the most important type of loss caused by defective IT services. Secondly, it may be quite difficult to prove and quantify the losses suffered.

¹⁸⁷ Siemerink 2007: 21-23.

¹⁸⁸ Siemerink 2007: 101: "spant zich als een goed dienstverlener in zorg te dragen voor".

¹⁸⁹ Siemerink 2007: 106-107, 241-244.

¹⁹⁰ Siemerink 2007: 232-233, 237, mentioning measures such as screening e-mail, providing information on the importance of anti-virus software, informing about malware infections.

¹⁹¹ Siemerink 2007: 260, 275-276, who makes an exception for damages resulting after consulting a helpdesk (p. 276).

Given the difficulties in obtaining an award of damages, and the desire to have effective remedies, corporate clients regularly prefer to enter into contracts in the form of Service Level Agreements (SLAs).¹⁹² An SLA typically specifies precise service levels (such as x hours response time to problems; 99,x% uptime of communication/servers), which makes it clear what the contractually obligated results are. Furthermore, an SLA should, if properly constructed, connect precise consequences to a failure to meet the agreed upon service levels. These consequences are usually formulated as financial consequences, either in the form of return payments and price reductions, or (if service levels are exceeded) in the form of bonus payments. However, there are as of yet no indications that SLAs contain stipulations regarding preventive measures to combat cybercrime.

5.2.2.4. *Businesses*

With respect to businesses that are the victim of DDoS attacks: insofar as the victims are unable to meet their contractual obligations because of an attack, the precautions and countermeasures they have taken may be relevant to determine whether they are in breach, either because of fault or because of lack of care (or possible because such an attack is not considered to be force majeure). However, at present this usually does not lead to liability, particularly because of restrictive contractual guarantees and exclusion clauses on recoverable damage.¹⁹³

Insofar as a business has been the victim of security breach, possibly leading to ransomware infection, the business will have to notify the individuals concerned (s. 5.2.4). Such a security breach may constitute a tort to the individuals whose data has been leaked.¹⁹⁴ However, it is hard to assess an appropriate amount of damage. Moral damages (art. 6:106 BW) might be awarded because the security breach infringes the fundamental right of privacy.

5.2.2.5. *Others*

There are few indications of the possible liability of other Internet organisations involved with the administration of Internet. Registrars are organisations that register domain names and keep administration about the 'owners' of the domain names. Theoretically, they may be found liable if they could have prevented damage by taking appropriate care. However, we have not found that such an action has actually been instigated, possibly due to the fact that registrars only register domains and do not have a duty to monitor what is done with or through the domain. Other IT organisations are involved in setting the

¹⁹² Cf. Drion & De Wit 2005.

¹⁹³ Tjong Tjin Tai 2013, as regards liability of banks towards their customers.

¹⁹⁴ Baas & Van Rest 2012.

protocols that determine how the Internet operates. Although these protocols influence the possibility and spread of cybercrime, this in itself will not lead to (tort) liability. The mere fact that a facility can be abused does not make its availability unlawful, in particular as the victims of the facility make use of it voluntarily.

5.2.3. *Criminal law*

The Dutch Criminal Code (Wetboek van Strafrecht, hereafter WvSr) dates from 1886 and is frequently adapted and updated to keep pace with developments in crime and society. There are two types of offences: crimes (misdrijven) and misdemeanours (overtredingen). The Criminal Code only uses maximum penalties but not minimum penalties. An important characteristic of Dutch criminal law is the right to exercise prosecutorial discretion (opportuniteitsbeginsel): the public prosecutor (Officier van Justitie) decides whether or not it is expedient to prosecute someone for an offence. As a result, criminal provisions can be formulated rather broadly, covering acts that may not necessarily be very worthy of criminal prosecution. Therefore, although some actions by e.g. ISPs or end users might be classified as an offence in theory, they may not be treated as an offence in practice.

The Criminal Code has been adapted repeatedly to catch up with new forms of cybercrime,¹⁹⁵ in particular through the Computer Crime Act (Wet computercriminaliteit) of 1993¹⁹⁶ and the Computer Crime II Act (Wet computercriminaliteit II) of 2006.¹⁹⁷ The Convention on Cybercrime (see s. 7.3) has been fully implemented in the WvSr. Directive 2013/40/EU of 12 August 2013 on attacks against information systems (see s. 7.3) is currently being implemented by raising penalties for various forms of cybercrime,¹⁹⁸ while a new Computer Crime III Bill (Wetsvoorstel computercriminaliteit III) is being prepared that would, inter alia, criminalize receiving (heling) of data.¹⁹⁹

5.2.3.1. *Possible types of duties of care*

In Dutch criminal law, one can distinguish four forms of criminal liability that are related to the concept of duties of care. The first type is offences based on negligence. Generally, criminal liability is imposed only in cases of intentional actions (dolus); the lower threshold of criminal intent (conditional intent, *voorwaardelijk opzet*) does not require someone to make a conscious and deliberate choice to create an effect, but rather to consciously

¹⁹⁵ Koops 2010 provides a general overview, also Koops 2014.

¹⁹⁶ Staatsblad 1993, 33. The Staatsblad is the official journal in which all Dutch laws and most decrees are published.

¹⁹⁷ Staatsblad 2006, 300.

¹⁹⁸ Kamerstukken II [Parliamentary Documents, Second Chamber] 2014/15, 34 034, nrs 1-3.

¹⁹⁹ Wetsvoorstel computercriminaliteit III, May 2013, version for public consultation available at <http://www.internetconsultatie.nl/computercriminaliteit>.

accept a considerable likelihood that a certain effect will take place. But besides intentional offences, there are also offences based on blameworthiness (*schuld* or *culpa*), which are attributable to offenders who have not been sufficiently careful and thus caused an effect, e.g. someone's death or severe injury, to happen. The general yardstick for *culpa* is that someone has not acted as considerably as can be expected of the average person in certain situations. Thus, negligence-based offences clearly constitute a type of duty of care in criminal law.

The second type are omission crimes, in which someone is criminally liable for not acting in situations in which an act or intervention was expected. These are rare: they are limited to situations in which an action could prevent grave consequences and would not be very difficult or demanding, for instance, not providing help to someone in acute danger of dying while helping would not reasonably be dangerous for the helper (art. 450 WvSr, a misdemeanour punishable with maximum three months' imprisonment). This category is not relevant for cybercrimes, at least not in the form of offences defined explicitly as omissions. Not acting might under certain conditions be qualified as an offence under a 'commission' crime if the result is attributable to the nonactor. An example could be the Chief Information Security Officer (CISO) of an electricity company who is informed of a serious bug in SCADA software used in the infrastructure and of announcements by activist groups that they aim to perform cyber-attacks on utility companies; if the CISO refrains from actions to repair the bug and an attack subsequently takes place, he might be held liable for negligently causing damage to electrical infrastructure resulting in the hindering of electricity provisioning (art. 161ter WvSr). Since this is a negligence-based offence, it is an example of the first type rather than the second.

The third type are forms of aiding and abetting. Dutch criminal law has various forms of accessory crimes, ranging from causing (*doen plegen*) or inciting (*uitlokken*) someone to commit a crime or jointly perpetrating a crime (*medeplegen*) (art. 47 WvSr) to being an accomplice of the crime (art. 48 WvSr, *medeplichtigheid*). The latter includes intentionally helping someone to commit a crime and intentionally providing opportunity, means, or information to commit a crime. The combination of aiding and conditional intent (the lower threshold of intent) approximates, to some extent, a duty of care, in the sense that people who knowingly accept the likelihood that what they are doing provides others with an opportunity to commit a crime, implies a certain duty to be aware of the consequences of one's actions and possibly to take preventive measures to diminish the opportunity to commit crimes. However, the threshold for *medeplichtigheid* is still high and closely related to the foreseeability that a particular criminal result will happen through the opportunity that one provides. The combination of aiding and conditional intent therefore remains rather far removed from a duty of care as understood in this report.

A particular form of accessory liability in relation to cybercrimes is the liability of ISPs

for criminal content. Dutch law provides an exception to the criminal liability of ISPs if they do all that can reasonably be asked of them to ensure that the data are made inaccessible, in response to an order from the public prosecutor based on a warrant from the investigating judge (art. 54a WvSr).²⁰⁰ The provision has flaws and is being revised in the Computer Crime III Bill, but since content crimes are outside the scope of this report, we will not discuss this further.

The first three types discussed so far all impose, to some extent, a duty on people to act in a certain way if they want to avoid being held criminally liable for results caused by themselves or others. Duties of care can, however, also take the form of certain conditions that have to be met in order for certain conduct to constitute a criminal offence, if these conditions imply a certain standard of behaviour for potential victims. This can be considered a fourth type of duty of care embedded in criminal law. A primary example is found in cybercrime law, under which hacking (unlawful access to a computer system or part thereof) can be criminalized only if security measures have been infringed.²⁰¹ In 1993, the Dutch legislator considered hacking punishable only if someone infringes a security measure or otherwise enters a computer by devious means (art. 138a-old WvSr, now art. 138ab WvSr). The security requirement was considered relevant as an incentive to encourage people and companies to protect their computers, something which many did not consider self-explanatory in the early 1990s. The standard of security was not particularly high: a minimal level of security was considered sufficient, meaning that some sort of protection had to exist: not merely a sign saying “do not trespass.” In other words, victims should not complain that their computers are hacked if they have not done anything to prevent access by unauthorized persons, but they do not have to have state-of-the-art protection. In 2006, however, the legislator decided to abolish the security requirement altogether (arguing that this was necessary to comply with international obligations under the Convention on Cybercrime and the Framework Decision on attacks against information systems, the precursor of Directive 2013/40/EU). It did so through the Computer Crime II Act, which renders punishable any form of unlawfully “entering” a computer as such, which removes from criminal law the incentive for end users to protect their computers. The literature considers this a missed opportunity.²⁰² Since Directive 2013/40/EU, which aims to harmonize the definitions of cybercrimes in the EU, criminalises hacking only if security

200 Den Dekker & Van der Linden-Smith 2014: 267.

201 See art. 2 Convention on Cybercrime: ‘Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intention-ally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures (...)’ (emphasis added).

202 Koops 2010, p. 7.

measures are infringed,²⁰³ the question can be raised whether Dutch law should be changed to reinstall the security requirement as a condition of hacking in art. 138ab WvSr. This would (re)establish a duty of care, albeit a minimal one, on end users to have some basic protection on their computers, in the sense that they cannot complain about hacking if they have not complied with this standard.

5.2.3.2. *Duties of care for the three topics of cybercrime*

In this report we focus on three problems associated with cybercrime in particular. Does Dutch law impose any duty of care on suppliers, ISPs, or users to do something about these problems?

1) *Ransomware* can be classified under various criminal provisions. Various computer-integrity crimes can apply: hacking²⁰⁴ (art. 138ab WvSr), spreading malware (art. 350a para. 3 WvSr), and particularly data interference (art. 350a para. 1 WvSr), since the ransomware blocks the data on the infected computer by encrypting it. A number of computer-assisted crimes could also apply if victims actually pay a ransom, in particular computer-related extortion: forcing someone to give away a good (i.e. money) by threatening to block or delete computer data (art. 317 para. 2 WvSr). This crime is punishable with maximum nine years' imprisonment. (Alternatively, if ransomware is conceptualized as devious rather than violent, the crime of fraud applies: inducing someone through cunning artifice (*listige kunstgrepen*) to give away a good, art. 326 WvSr; punishable with up to four years' imprisonment.) If victims do not (yet) pay a ransom, the infection itself together with the request to pay a ransom could constitute attempted extortion or attempted fraud (art. 45 juncto 317 para. 2 or art. 326 WvSr, punishable with a maximum penalty that is a third less than the crime itself). All of these crimes require intent, however, and will only apply to the perpetrators of the ransomware.

²⁰³ Art. 3 Directive 2013/40/EU ('when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by in-fringing a security measure, at least for cases which are not minor', emphasis added).

²⁰⁴ It can be questioned whether causing malware to be installed on a victim's computer constitutes unlawful access to that computer, since there is no direct connection between the offender and the victim's computer through which the offender can access the contents of that computer. However, case-law has established that sending out viruses that infect computers also constitutes hacking (HR 22 February 2011, ECLI:NL:HR:2011:BN9287).

There is, however, also a negligence variant of data interference: art. 350b para. 1 WvSr penalizes someone who is to blame (*aan wiens schuld te wijten is*) for causing data to be unlawfully changed, deleted, or blocked, if this results in serious damage to those data; this is punishable with a maximum of one month imprisonment.²⁰⁵ Similarly, art. 350b para. 2 WvSr criminalizes negligence that causes the spreading of malware: ‘He who is to blame for data being unlawfully made available or spread that are intended to cause damage in a computer, shall be punished with imprisonment of at most one month or a fine of the second category.’²⁰⁶ Ransomware is a form of malware in this sense, since it is intended to cause damage in the computer by encrypting the data so that the user can no longer access the data. Both crimes—negligent data interference and negligent spreading of malware—would be committed by third parties, such as ISPs, providers of anti-virus software, or system administrators, if the infection of an end-user’s computer can somehow be blamed to them.

At what point intermediaries can be blamed for causing computers to be infected with malware is not clear, however: there is no case-law on this. It is only briefly discussed in the literature. Stamhuis points out that the ‘negligent version of malware distribution might only apply to professionals and not to ordinary end users from whom we may not expect the required level of security’ (and noting that the distinction between professionals and end users needs to be reflected upon in the web 2.0 context); he does not, however, provide further criteria when (professional) intermediaries could be held liable under article 350b WvSr.²⁰⁷

One could argue that if a particular form of ransomware is well-known in the security community and can be easily and reliably recognized by filters, access providers who do not filter out messages in which this ransomware is embedded (in an attachment) are partly to blame for the end-user’s computers being infected. But before such a claim can be made, it should be established that the filtering lies within the access provider’s capacity (in terms of technical capability and resources) and is lawful and overall socially desirable (it should not require, e.g., Deep Packet Inspection, an intrusive form of ISP interference that cannot

205 ‘Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, wordt, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt, gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.’

206 ‘Hij aan wiens schuld te wijten is dat gegevens wederrechtelijk ter beschikking gesteld of verspreid worden die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.’ (our translation)
A fine of the second category is maximum 4,050 EUR (art. 23 WvSr).

207 Stamhuis 2012, p. 21.

be imposed on them as a duty of care). Similar questions arise under civil liability (see sections 5.2.2.2 and 7.4), and since generally speaking, the standard for blaming someone for not taking sufficient care is lower in private law than in criminal law (as the blame in criminal law carries a stigma of a moral wrong, which is not necessarily the case with blame in private law), we refer to the discussion there. Only if a duty of care for ISPs to filter out malware can be construed under private law, can we consider whether and to what extent this duty of care also carries over to criminal law as an obligation under art. 350b WvSr to avoid the infection of users' computers. Finally, the aforementioned art. 54a WvSr excludes criminal liability for ISPs who remained passive. Given these rules and complications, for the time being we consider the challenges of filtering malware too complicated to impose a duty of care on ISPs under criminal liability for negligent data interference or spreading of malware.

For anti-virus software providers, it could be somewhat easier to argue that they are (partly) to blame for end-user computers being infected if their software does not recognize a well-known instance of malware, including ransomware; after all, their purpose is to filter out malware, and end users rely on them to recognize known threats. But again, it is less likely to assume criminal liability than civil liability here, and civil liability for negligence by anti-virus software providers is already a dubious issue.²⁰⁸ Moreover, prosecuting an anti-virus software provider under art. 350b WvSr for negligently causing users' computers to be infected by known malware, which the public prosecutor could attempt in order to set an example and to elicit a standard of care in this area, would probably have various counter-productive effects: anti-virus software providers would include the strongest possible exoneration clauses in their terms and conditions in order to lower the standard of care that customers could legally expect from them, and they could raise their prices significantly to account for the increased risk of criminal liability (which might reduce the number of consumers that install anti-virus software), or they might even withdraw from the Dutch market altogether.

Holding ISPs or anti-virus software providers criminally liable for negligent data interference seems to be several steps too far in the current state of affairs. The only situation of negligent data interference that appears somewhat realistic concerns cases in which individuals in professional settings are grossly negligent, thereby causing computers within their organizations to be seriously damaged. If system administrators, particularly in large organizations that employ expert professionals to run their systems, fail to take measures to prevent ransomware from infecting corporate computers while such measures would have been expected of average professionals in the field, the computer infection can be blamed on them. (The blame would also attach to end users who caused a particular com-

208 See s. 5.2.2.2 on liability of software vendors, which fully applies to anti-virus software as well.

puter to be infected, for instance by opening an infected attachment to an email message, but for average users in organizations, this would be dealt with under private law rather than under criminal law.) System administrators are in a position in which they have taken up a responsibility to secure computers in their organization, and the criminal law doctrine of the *Garantenstellung*²⁰⁹ can be used in such situations to argue that they have to comply with higher standards of conduct than average users; hence, criminal liability for negligent behaviour is easier to assume for individual professionals in the field of information security. (And, depending on the hierarchy and distribution of responsibilities within an organization, the CISO or other executives ultimately responsible for the information security might also be held liable if the criteria for criminal liability for functional leadership of a crime committed by employees²¹⁰ are met.) However, prosecution for negligent data interference seems only reasonable in cases where system administrators (or their responsible managers) were obviously grossly negligent; in cases of ransomware (and similar malware), this would apply only to malware that is well-known and sufficiently easy to recognize and block, given the resources available.

To sum up, there is a certain duty of care embedded in Dutch criminal law in relation to ransomware, but this duty applies only to expert information security professionals in organizational settings, and the standard of care is fairly low. In fact, any information security professional should use readily available tools to prevent well-known malware from infecting computers to be worth her job in the first place. Criminal law therefore does not offer a substantial additional standard of care over and above basic job requirements in this respect.

2) DDoS attacks are primarily criminalised in art. 138b WvSr as ‘the intentional and unlawful hindering of the access to or use of a computer by offering or sending data to it’, which is punishable by up to one year imprisonment or a fine of the fourth category.²¹¹ In the bill which implements Directive 2013/40/EU, the maximum penalty is raised to two years’ imprisonment, and to three years’ imprisonment if the DDoS attack takes place using a botnet or five years’ imprisonment if the DDoS attack causes serious damage or is directed against a computer belonging to the vital infrastructure.²¹² System interference (including DDoS attacks) of computers and computer networks that are used for the com-

209 Noyon/Langemeijer & Rummelink, *Wetboek van Strafrecht*, (looseleaf), Inleiding, aant. 9.

210 See HR 23 February 1954, NJ 1954/378.

211 ‘Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.’ (our translation) A fine of the fourth category is maximum 20,250 EUR.

212 Kamerstukken II 2014/15, 34 034, no. 2.

mon good is also punishable under another provision, if the system is impeded or if the interference causes general danger (*gemeen gevaar*) to goods, services, or people (art. 161sexies WvSr). All of these crimes require intent, however, and will only apply to the perpetrators of the DDoS attacks.

As with malware, there are also two provisions criminalising negligent system interference, but they are limited to systems that have a public function. Art. 161septies WvSr stipulates the following:

‘He who is to blame that any computer or telecommunications system is destroyed, damaged, or made unusable, that an interference in the course or functioning of such a system occurs, or that a security measure taken with respect to such a system is prevented, shall be punished:

- 1°. with imprisonment of at most six months or a fine of the fourth category, if thus the storage, processing, or transmission of data for the common good is blocked or impeded, a public telecommunications network or the execution of a public telecommunications service is disrupted, or common danger to goods or service delivery is caused;
- 2°. with imprisonment of at most one year or a fine of the fourth category, if thus danger to another’s life is caused;
- 3°. with imprisonment of at most two years or a fine of the fourth category, if the act causes someone’s death.’²¹³

213 ‘Hij aan wiens schuld te wijten is dat enig geautomatiseerd werk of enig werk voor telecommunicatie wordt vernield, beschadigd of onbruikbaar gemaakt, dat stoornis in de gang of in de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld, wordt gestraft:

- 1°. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie, indien daar door verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ten algemenen nutte, stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, of gemeen gevaar voor goederen of voor de verlening van diensten ontstaat;
- 2°. met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie, indien daardoor levensgevaar voor een ander ontstaat;
- 3°. met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie, indien het feit iemands dood ten gevolge heeft.’ (our translation)

Article 351bis WvSr similarly penalizes negligent system interference of computers and telecommunication systems that are used for the common good (*ten algemenen nutte*), regardless of whether there is actual hindering of a public service or risk to life—the mere negligent interference with a ‘common good’ computer suffices.²¹⁴ The penalty for this crime is at most one month imprisonment or a fine of the second category.

These provisions are relevant for DDoS attacks on public computer systems, since they imply that not only the perpetrators of DDoS attacks on public systems themselves, but also people who have acted with gross negligence to allow (or not prevent) such attacks can be prosecuted, particularly if public systems are seriously disrupted or if a risk to public goods or to life is involved. This is the case for vital infrastructures (energy, water, banking, the public telecommunications network) and government services (e.g. DDoS attacks on the website of the tax administration), but also for attacks on, for instance, hospitals. It should be noted, however, that DDoS attacks usually block public websites, but not back-office data processing, so that most DDoS attacks will not disrupt public services or involve risk to life. Nevertheless, the unavailability of certain websites, such as Internet banking services, can cause serious disruption of public service provisioning, so that DDoS attacks on these could be classified as data interference with common endangerment.

This raises the question to what extent intermediaries, such as ISPs, or professionals responsible for information security in public-sector organizations or otherwise associated with the common good (including financial and medical service providers), can be held liable if they have been grossly negligent in preventing DDoS attacks. We think that the same arguments apply here as in the case of ransomware and therefore refer to the analysis above. The same conclusion can be drawn here: holding intermediaries liable for negligently causing system interference through DDoS attacks is one or two steps too far. One could at most, on the basis of a *Garantenstellung* argument, consider holding liable expert information security professionals in organizational settings who have acted grossly negligently under art. 161septies WvSr. The situations do differ, however, in at least one respect. It may be reasonable to expect information security professionals to prevent infection with well-known malware (since it does not cost much effort or resources to ensure this by applying existing measures), which is largely a matter of applying a knowledge standard. It is, however, less reasonable to expect information security professionals to prevent DDoS attacks, since the prevention of this type of cybercrime requires resources (investing in more computer power) rather than the application of certain knowledge. Information security professionals could only be considered to have acted grossly negligently in terms of

214 ‘Hij aan wiens schuld te wijten is dat enig in het vorig artikel bedoeld goed of werk, vernield, be-schadigd, onbruikbaar gemaakt, onklaar gemaakt of weggemaakt wordt, wordt gestraft met hechtenis van ten hoogste een maand of geldboete van de tweede categorie.’

criminal law if they have not taken basic measures to stop even small-scale DDoS attacks.

Another question regards whether end users who have allowed their computer to be infected with malware and thus to become part of a botnet that is used for DDoS attacks, could also be blamed for negligently causing system interference. This question can be easily answered negatively, for three reasons. First, (the computer of) an individual computer user only contributes to a small fraction to the attack, so it can hardly be said to cause the attack. Second, the standard of care that can be expected of computer users to prevent their computers from being infected with botnet malware is much lower than the standard for information security professionals. And third, even if end users could be blamed to some extent for having allowed their computers to become part of a botnet and thus endangering, to some extent, the computers of other users, it is hardly foreseeable for which purpose the botnet would be used (since botnets can serve very many functions). The end user could not be expected to foresee that they would contribute to attacks on computers *with a public function* in particular.

3) *Security of software and hardware* is not a type of cybercrime in itself and it is not easily associated with a particular form of crime. Bugs in software or hardware can be employed for various cyber-attacks, but the connection between the bug and a particular cyber-attack is very thin in terms of causality and foreseeability. Where the connection between intermediaries and ransomware or DDoS attacks is already tenuous from the perspective of negligence-based crimes, the connection between software and hardware suppliers and cybercrimes is surely even weaker. Thus, although one could theoretically discuss whether providers of mass-market software or hardware with extremely poor security could be prosecuted under the negligence crimes of 161septies, 350b, or 351 WvSr, we do not think any Dutch prosecutor would seriously consider initiating such a prosecution.

One type of criminal offence relates specifically to security of hardware and software: the criminal misuse of devices (art. 6 Convention on Cybercrime, implemented in Dutch law in art. 139d para. 2 and 161sexies para. 2 WvSr, and in art. 350d of the proposed bill implementing Directive 2013/40/EU). Simply put, this criminalizes activities in preparation of cybercrimes in the form of, inter alia, creating, making available, or possessing hardware or software that can be used to commit a cybercrime. Two conditions limit the criminal liability, however: the hardware or software needs to be primarily developed or adapted to commit a cybercrime, and the creation etcetera needs to occur with the intent that it be used to commit a cybercrime. For these reasons, this offence does not put a duty of care on hardware or software providers to ensure some level of security in their products, since one may assume that these providers do not develop their products primarily for the purpose of committing crimes.

5.2.4. Administrative law

Additional obligations may derive from other public law statutes. In particular telecommunication law imposes various obligations.²¹⁵ The Dutch Telecommunication Statute (*Telecommunicatiewet, Tw*) derives partly from the Directive 2002/21/EC of 2002 on a regulatory framework for electronic communications (Framework Directive). We will focus only on ISPs.

ISPs have to respect the principle of net neutrality.²¹⁶ This holds that Internet Service Providers may only block or delay the traffic to and from specific Internet services or applications insofar as this is necessary for explicitly specified purposes, including the “integrity and security of the network and the service of the provider in question or the accessory machine of the end user” (art. 7.4a(1)(b) Tw) or compliance with a specific statutory obligation or judicial order (art. 7.4a(1)d Tw). In case the infringement of integrity or security of the network or service or an accessory machine of the end user, as meant in art. 7.4a(1)(b) Tw, is caused by traffic from an accessory machine of the end user, the provider has to inform the end user before blocking or delaying the traffic in order to allow the end user to stop the infringement.²¹⁷ If the urgency of intervention does not allow prior notice, the notice has to be provided as soon as possible. There is uncertainty as to whether this obligation also holds for providers of free WiFi services.²¹⁸ ISPs may provide additional filtering services, but these may not be made semi-mandatory by, for example, asking higher prices or lower quality for unfiltered services.²¹⁹

ISPs are further subject to several obligations regarding cybersecurity.²²⁰ They generally have to take measures to ensure continuity of service (chapter 11A Tw, art. 11a.1(2) Tw). In case of significant disturbance of availability the ISP has to notify the Ministry of Economic Affairs (art. 11a.2(1) Tw).²²¹

Furthermore, ISPs have to take measures for security. On behalf of the privacy of users, they have to take appropriate technical and organisational measures to safeguard the security and safety of the networks and services offered. The measures are to guarantee – taking into account the state of technology and the costs – a fitting level of security, proportionate to the risk involved (art. 11.3(1) Tw). They similarly have to take appropriate measures to control the risks for security and integrity of their networks (art. 11A.1 Tw). ISPs

²¹⁵ Gijrath a.o. 2014, Zwenne & Knol 2014.

²¹⁶ Art. 7.4a Tw.

²¹⁷ Art. 7.4a(2) Tw. This obligation only applies to end users of the provider in question, not end users of other providers.

²¹⁸ Gijrath a.o. 2014: 143.

²¹⁹ Gijrath a.o. 2014: 144.

²²⁰ Gijrath a.o. 2014: 148-149.

²²¹ See <https://www.meldplichttelecomwet.nl>.

furthermore have to inform users of special risks for security of the network or service offered, and of preventive means (and connected costs) other than those which the provider has to take himself (art. 11.3(3) Tw). In case of an infringement of the security, the provider has to inform both the Dutch Consumer and Market Authority (*Autoriteit Consument en Markt*, ACM) (art. 11.3a Tw)²²² and the users whose privacy might be infringed (art. 11.3a(2) Tw).²²³

ISPs are prohibited from checking, tapping and listening to communication and related data,²²⁴ but an exception applies insofar as such acts are necessary for maintaining the integrity and security of the networks and services of the provider.²²⁵ ISPs may not store traffic data beyond what is necessary for provision of the services, but an exception applies to forensic investigation (*opsporen*) of fraud (art. 11.5(5) Tw). ISPs have to store traffic data for police and security services (art. 13.2a Tw).²²⁶

Businesses have a general obligation to treat personal data securely.²²⁷ A breach of security that involves unauthorised access to personal data may be a violation of data protection rules. Furthermore, the ePrivacy Directive 2002/58/EC²²⁸ requires member states to implement a notification duty for all businesses²²⁹ in case of a personal data breach.²³⁰ These rules require notification to the competent national authority²³¹ as well as to the individuals concerned. A legislative proposal to implement this duty is pending.²³²

Supervision of telecommunication obligations is performed by the ACM²³³ and the Ministry of Economic Affairs.²³⁴ Service providers offering public access to electronic communication networks or services have to register with the ACM (art. 2.1 Tw). As of Decem-

222 See <https://www.meldplichttelecomwet.nl>.

223 Borgesius 2011.

224 Art. 11.2a(2) Tw.

225 Art. 11.2a(2) (b) Tw.

226 The provision is based on the Data retention Directive 2006/24/EC. After ECJ 8 April 2014, cases C-293/12 and C-594/12, which declared this directive invalid, there is uncertainty as to the validity of this provision (Gijrath a.o. 2014: 154, 163-167).

227 See the detailed rules in the Wet bescherming persoonsgegevens (Law on protection of personal data, the implementation of the Privacy Directive 95/46/EC). Further relevant is the ePrivacy Directive 2002/58/EC, updated by the Directive 2009/136/EC. See Berkvens & Prins 2014.

228 As revised by Directive 2009/136/EC.

229 This is to be distinguished from the aforementioned notification duties for ISPs.

230 Art. 4(3), after revision by Directive 2009/136/EC. See further EU Regulation 611/2013 on the measures applicable to the notification of personal data breaches.

231 In The Netherlands these are the Dutch Data Protection Authority (College bescherming persoonsgegevens) and the Authority for Consumers and Markets (Autoriteit Consument en Markt).

232 Parliamentary Documents nr. 33.662. The legislative proposal has been accepted by the Second Chamber of Parliament at 10 February 2015.

233 Art. 15.2 Tw.

234 Art. 15.1 and 1.1(a) Tw.

ber 2014, more than 700 providers of electronic communication networks and more than 700 providers of electronic communication services were registered.²³⁵ These do not all involve Internet related services.

5.2.5. Conclusion

Dutch law provides a basis for assuming some duties of care and diligence for the actors under consideration here. ISPs as well as software vendors have such duties to their contractual relations. However, the extent of these duties is usually contractually limited to a large extent, while contractual limitation clauses reduce the possibility of enforcement through damage claims to practically zero. As regards tort liability, ISPs who remain passive cannot be held liable, while there is little indication that software vendors can be held liable by third parties for negligence because of software vulnerabilities. Businesses may however be liable to some extent for unavailability of services or security breaches. Criminal liability could theoretically be assumed in certain cases on the basis of aiding and abetting cybercrime, but in practice the requirements for such liability would not usually be met. Administrative law further limits the discretionary room for ISPs to take preventive action against cybercrime, by complicating actions such as traffic inspection and disconnecting users.

5.3. United States of America

5.3.1. Introduction

The United States of America (U.S.A.) is a federation of states. Only federal law applies to the whole of the United States. To a large extent, the law is still mainly formed at the state level, where the states have their own legal system. The majority of these states have a common law system, because of which private law is to a large extent formed by precedent.²³⁶ However, common law has had to give way to extensive legislative activity in many cases, as a result of which much of state and federal law is nowadays statutory law. In particular the state of Louisiana has a civil code inherited from the French civil code; furthermore California has a civil code, which is admittedly mostly a codification of common law rules without the strict systematic ordering that characterises most codified systems. Specific topics are often regulated by specific codes, both at the state level and federal level.

²³⁵ Register at acm.nl.

²³⁶ Von Mehren 1988: 3, Raaijmakers 2002: 122.

5.3.2. *Private law*

5.3.2.1. *General contract law*

Contract law in the U.S. is generally state law instead of federal law.²³⁷ Consequently, the states have their own law, but the differences generally only regard details.²³⁸ The differences are further reduced because of the influence of case law, which has a harmonising effect: courts in the different states may for their interpretation of state law look at developments in other states. Additionally, there have been efforts at harmonisation, in particular through several sets of Restatements of the Law, compiled and published by the American Law Institute (ALI) on the basis of research of many precedents.

Relevant to software are the ALI Principles of the Law of Software Contracts, which attempt to unify the law for software contracts.²³⁹ The purpose of the ALI Principles is to ‘draft legal principles to guide courts in deciding disputes involving transactions in software and to guide the drafting of software contracts’.²⁴⁰ The ALI Principles may become part of the law of a state jurisdiction if a state court adopts them in case law.²⁴¹ The drafters of the Principles of the Law of Software Contracts aimed primarily at summarizing existing law.²⁴²

Finally, there are initiatives towards creating harmonised statute law. An important example is the Uniform Commercial Code (U.C.C.), which has been adopted by many states, albeit sometimes only in part.²⁴³ For example, California has adopted articles 1 to 9 U.C.C.²⁴⁴ U.C.C. governs commercial business transactions. Particularly, the U.C.C. covers transactions regarding goods. Mass-market standard software is considered a good under the U.C.C., even though it is inherently intangible.²⁴⁵

With regard to computers, there have been two initiatives similar to the U.C.C. The Uniform Computer Information Transactions Act (UCITA)²⁴⁶ and the Uniform Electronic

²³⁷ Farnsworth 2010: 134, Reitz & Carlson 2002: 282.

²³⁸ Farnsworth 2010: 134.

²³⁹ Moringiello & Reynolds 2010: 2, Rustad & Onufrio 2010, also response from the reporters: Hillman & O’Rourke 2010.

²⁴⁰ https://www.law.stanford.edu/sites/default/files/project/205170/doc/slspublic/DeWerra_Abstract_ttlf.pdf

²⁴¹ Hillman & O’Rourke 2010: 1519.

²⁴² This is also recognised by Moringiello & Reynolds 2010: 12 (with some exceptions identified earlier) and Rustad & Onufrio 2010: 46. The ALI expect the drafters of Principles, where required, to state the law as it should be, cf. Moringiello & Reynolds 2010: 6, referring to <http://www.ali.org/doc/StyleManual.pdf>, p. 12.

²⁴³ The list of states is available at: <http://uniformcommercialcode.uslegal.com/states-adopting-the-ucc/>

²⁴⁴ <http://uniformcommercialcode.uslegal.com/states-adopting-the-ucc/california/>

²⁴⁵ Moringiello & Reynolds 2010: 3, Childers 2008: 146, Horovitz 1985. See also the discussion in Rustad & Onufrio 2010, par. B, p. 29-33. Contra: Brennan 2000.

²⁴⁶ About the UCITA see Brian D. McDonald, ‘The Uniform Computer Information Transactions Act’, *Berkeley Technology Law Journal* 2001: 461-484.

Transactions Act (UETA)²⁴⁷ were drafted in order to adapt contract law to technological developments.²⁴⁸ UCITA applies to ‘computer software, multimedia products, computer data and databases, online information, and other such products.’ It contains provisions such as to the binding force of shrink-wrap licenses, the presence of implied warrants for defects, and the possibility of liquidation of damages. Although UCITA aims at providing a balance between the interests of software vendors and consumers, in practice the balance may tilt towards the vendors because the binding force of shrink-wrap licenses can be used to exclude the default rules of consumer protection. Concerns about the lack of consumer protection against poorly designed software motivated a strong lobby against accepting UCITA.²⁴⁹ As a result only Virginia and Maryland have adopted the act.²⁵⁰ Given this lack of recognition, UCITA has no practical relevance. We will refer to it occasionally, if it is indicative of legislative trends. Part of the provisions of UCITA have influenced the ALI Principles on Software Contracts.²⁵¹ The UETA aims at regulating electronic transactions, and is not relevant for the present research.

The general duties of care and diligence under contract law, as well as the available remedies, can be derived from the general structure of U.S. and California contract law.

The word ‘contract’ is used ‘to mean a promise, or a set of promises, that the law will enforce or at least recognize in some way’.²⁵² In general, a promise is interpreted as an undertaking to reach a specific result.²⁵³ A contract is formed by offer and acceptance. Acceptance is the final step in establishing a contract.²⁵⁴ Acceptance usually occurs in the form of a promise, although acceptance by performance is also possible.²⁵⁵

A peculiarity of common law is that valid contracts also require the presence of consideration: something provided in return for the promise of the other party. The offeror could seek as consideration a return promise (a bilateral contract) or performance (a unilateral contract).²⁵⁶ Consideration for a promise could entail ‘virtually anything’ to bargain for.²⁵⁷

247 <http://www.ncsl.org/research/telecommunications-and-information-technology/uniform-electronic-transactions-acts.aspx>

248 Bernstein 2002: 160.

249 Shah 2000: 92, Rustad & Onufrio 2010, par. E: 37-40, also <http://cpsr.org/prevsite/program/UCITA/ucita-fact.html/>. More information: <http://ubiquity.acm.org/article.cfm?id=355133>.

250 <http://www.ucitaonline.com/>

251 This is explicitly recognised where applicable in the comments to the ALI Principles.

252 Farnsworth 2004, volume 1, par. 1.1: 4. ‘A promise is a manifestation of intention to act or refrain from acting in a specified way, so made as to justify a promise in understanding that a commitment has been made’ (Restatement Second of Contracts § 2 (1)).

253 Farnsworth 2004, volume 2, par. 9.1: 586.

254 Farnsworth 2004, volume 1, par. 3.13: 269.

255 Farnsworth 2004, volume 1, par. 3.13: 270.

256 Farnsworth 2004, volume 1, par. 3.12: 265-266.

257 Farnsworth 2004, volume 1, par. 2.3: 79.

An example is the case of *Wood v. Lucy, Lady Duff-Gordon*, 222 N.Y. 88, 118 N.E. 214 (1917), in which consideration for ‘a duty to use reasonable efforts’ was found in the promise of exclusive representation.²⁵⁸ Purely gratuitous or gift promises are unenforceable for lack of consideration.²⁵⁹

Contractual liability requires the presence of an obligation that is breached. The most important contractual obligations are formulated as *warranties*. A warranty can be described as a statement or representation about the goods or services sold.²⁶⁰ The representation may for example involve affirmations of quality or quantity or title. Kopf distinguishes the following types of warranties: expressed warranties, remedies, express oral warranties, warranty invalidation, technical specification warranties and implied warranties.²⁶¹ The U.C.C. distinguishes between expressed (U.C.C. § 2-313) and implied warranties (U.C.C. § 2-314 and 315).²⁶² U.C.C. § 2-314 is about the implied warranty of merchantability and U.C.C. § 2-315 concerns the implied warranty of fitness for particular purpose.²⁶³ U.C.C. § 2-316 describes exclusions or modifications of warranties. In general, exclusion of a warranty is possible under strict conditions,²⁶⁴ which require adopting the requisite phrases.

Contractual liability may also follow from the violation of an obligation or duty of best efforts. This is important in the present context as this doctrine is analogous to the duty of care and diligence. In U.S. contract law, best efforts ‘is a standard that has diligence as its essence and is imposed on those contracting parties that have undertaken such performance.’²⁶⁵ The duty of best efforts is the counterpart of ‘appropriate means’ in French law.²⁶⁶ There are three ways in which a duty of best efforts could arise in a court case on contract law: an explicit contract term expressing that a promise only entails a duty of best efforts,²⁶⁷ interpretation of a contractual clause that expressly requires a specific result, and the imposition of a duty by constructing best efforts as an implied term.²⁶⁸ The term ‘best efforts’ is hardly mentioned in the U.C.C. or the Restatement on Contracts.²⁶⁹ It has been argued that

258 Farnsworth 2004, volume 1, par. 2.13: 137.

259 Farnsworth 2004, volume 1, par. 2.5: 85. Hillman & O'Rourke 2009: 5. Referring to Restatement Second of Contracts: § 3 (“A bargain is an agreement to exchange promises or to exchange a promise for a performance or to exchange performances.”).

260 Guarino 2002: 568.

261 Kopf 1987: 536-546.

262 Raaijmakers 2002: 135-136.

263 Alces 1999: 276-277.

264 Raaijmakers 2002: 141, Guarino 2002: 581-582, see U.C.C. § 2-316.

265 Farnsworth 2004, volume 1, par. 7.17c: 405. See further Coplan 2001.

266 Farnsworth 2004, volume 2, par. 9.1a: 588.

267 Referring to *Bloor v. Falstaff Brewing Corp.* 601 F.2d 609 (2d Cir. 1979).

268 Farnsworth 2004, volume 2, par. 7.17b: 402.

269 Farnsworth 2004, volume 2, par. 7.17c: 404. An examples is U.C.C. § 2-306(2) and the Second Restatement (introductory note chapter 11)

best efforts clauses will usually only allow limited awards of damages.²⁷⁰

In case of a breach of contract, there are various judicial remedies.²⁷¹ The most important remedy is damages. Damages is ‘the common form of relief for breach of contract’.²⁷² Not available for breach of contract are attorney’s fees, emotional distress damages and punitive damages.²⁷³ Another remedy is specific performance.²⁷⁴ This consists of an injunction to act in the manner required by the contract, i.e. to perform the contractual obligation. Specific performance is not always possible.²⁷⁵ A third remedy, the injunction, obliges the other party to refrain from certain actions rather than requiring him to perform certain actions.²⁷⁶ The remedy of restitution, finally, is ‘limited to cases in which the injured party has a claim for damages for total breach, so that that party’s remaining duties are discharged’.²⁷⁷

5.3.2.2. *General tort law*

Like contract law, tort law consists mainly of state law rather than federal law, with variations between different states. Although tort law is mostly based on case law, statutory law exists for particular topics.²⁷⁸ The California Civil Code regulates torts in sections 1708-1725,²⁷⁹ mostly codifying the rules developed in case law. California law recognizes a general duty of reasonable care if someone ‘creates a risk of harm of physical injury to another’.²⁸⁰

Of the available torts, negligence deserves particular attention: a ‘duty of care and diligence’ would usually be classified under U.S. tort law as negligence. The traditional elements for a cause of action for negligence are:²⁸¹

1. defendant owes plaintiff a duty of care,
2. a breach of this duty,
3. causation of harm,
4. defendant’s actions were the proximate cause of the harm, and
5. existence of damages based on a legally recognised kind of harm.

270 Tettenborn 2008: 313-314.

271 See also Guarino 2002: 573-574.

272 Farnsworth 2004, volume 3, par. 12.8: 189.

273 Bix 2012: 98.

274 Farnsworth 2004, volume 3, par. 12.5: 167. Referring to *Dalton v. Educational Testing Serv.* 663. N.E.2d 289 (N.Y. 1995)

275 Farnsworth 2004, volume 3, par. 12.5: 167-168.

276 Farnsworth 2004, volume 3, par. 12.5: 168.

277 Farnsworth 2004, volume 3, par. 12.19: 325.

278 Farnsworth 2010: 139.

279 <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1708-1725>

280 Cardi & Green 2008: 677. Referring to: Third Restatement : liability for physical harm § 7(a) & reporters’ note to cmt. a (Proposed Final Draft No. 1, 2005).

281 Dobbs 2000: § 114, p. 269.

More concisely, negligence may be defined as ‘the failure to live up to the standard of due care.’²⁸² For the required standard of care, the courts use ‘the care that would be exercised by a reasonable and prudent person under the same or similar circumstances to avoid or minimize risks of harm to others’.²⁸³ However, professional persons are ‘held to possess the skill and knowledge of others in good standing in their profession’.²⁸⁴ Negligence cases are heard by a jury. The jury has to decide whether the defendant met the required standard of care.²⁸⁵ Whether a duty of care exists, is decided by the court.²⁸⁶ It should be noted that under a negligence action economic loss and emotional distress do not enjoy the same level of protection as bodily and property integrity.²⁸⁷

Although both an action and an inaction may give rise to negligence, there are not treated the same.²⁸⁸ U.S. law distinguishes between misfeasance and nonfeasance, –‘between active misconduct working positive injury to others and passive inaction or a failure to take steps to protect them from harm’.²⁸⁹ In particular, for nonfeasance a special relation between parties is required, or an assumption of a duty to act, in order for the law to impose a duty to act.²⁹⁰ This amounts to hesitance in accepting liability for nonfeasance.²⁹¹ It is argued that this distinction is justified because misfeasance involves the creation of a new risk, while nonfeasance only leads to maintaining the status quo by not interfering on behalf of the victim.²⁹² It follows that there is no general duty to act nor a duty to rescue.²⁹³ A stranger does not have ‘the moral obligation of common humanity to go to the aid of another human being who is in danger, even if the other is in danger of losing his life’.²⁹⁴

282 Glannon 2005: 69.

283 Dobbs 2000: § 117, p. 277, also Keeton, Dobbs, Keeton & Owen 1984: 174 referring to *Vaughan v. Menlove*, 1837, 3 BingN.C. 468, 132 Eng. Rep. 490.

284 Dobbs 2000: § 122, p. 290, also Keeton, Dobbs, Keeton & Owen 1984: 185.

285 Farnsworth 2010: 140, Dobbs 2000: § 148.

286 Dobbs 2000: § 149, p. 355, Zekoll & Fleming 2002: 191.

287 Card & Green 2008: 677. Referring to Marc A. Franklin, Robert L. Rabin & Michael D. Green, *Tort Law and alternatives* 264 (8th ed. 2006).

288 Dobbs 2000: § 314.

289 Keeton, Dobbs, Keeton & Owen 1984: 373. Referring to Bohlen, *The Moral Duty to Aid Others as a Basis of Tort Liability*, 1908, 56 U.Pa.L.Rev. 217, 219.

290 Dobbs 2000: § 314, p. 853.

291 *Beau Baez III* 2014: 40. Referring to *Giggers v. Memhis Hous. Auth.* 277 S.W.3d 359, 364. (Tenn. 2009)

292 *Beau Baez III* 2014: 40. Referring to *Smith v. Anderson*, 72 P.3d 369, 372. (Colo. Ct. App. 2002)

293 *Beau Baez III* 2014: 41.

294 Keeton, Dobbs, Keeton & Owen 1984: 375. Some states have specific statutes that do impose a duty to rescue. See *De Villiers* 2004: 135. Referring to ‘*Handiboe v. McCarthy*, 151 S.E.2d 905 (Ga. Ct. App. 1966) (no duty to rescue child drowning in swimming pool); *Chastain v. Fuqua Indust., Inc.*, 275 S.E.2d 679 (Ga. Ct. App. 1980) (no duty to warn child about dangerous defect in lawn mower).’ The Second Restatement § 314 and 314A.

American law follows English law in this respect.²⁹⁵ However, a special relation between parties could create such a duty.²⁹⁶

A particular form of liability that deserves separate treatment in this report is product liability. Product liability is about ‘unreasonably dangerous products or products that are not reasonably safe for their intended uses’.²⁹⁷ Product liability as a general topic may be based also on contract, in particular breach of a warranty (of absence of defects). However, an action in tort is also available. Product liability as a tort has been formed through case law, which has been systematised by the Restatement (Second) of Torts (hereinafter Second Restatement) and later modified by the Restatement (Third) of Torts (hereinafter Third Restatement).²⁹⁸ It applies only to products and requires the presence of a defect, which need not have been known by the manufacturer. Doctrine recognises three categories for liability: manufacturing, design and warning defects.²⁹⁹ The effect of the Third Restatement is that for manufacturing flaws strict liability applies, while for design and warning defects something close to a negligence standard is used.³⁰⁰

There are two categories of cybertorts: torts against personal interests and torts against a personal property interest.³⁰¹ Torts against a property interest ‘have largely been recognized as actionable by most jurisdictions’.³⁰²

5.3.2.3. *Software vendors*

The law on software is complicated by the fact that it is not always directly clear whether there is a contract between vendor and user. The relationship between the software vendor and the user who has bought a copy of the software from the vendor is unquestionably of a contractual nature. A contract between vendor and user may also arise if the software is obtained or installed after clicking on an ‘accept’ button (either on the website from which the software was obtained, or during the installation process).³⁰³ In such cases, provided

295 Smits 2000: 10.

296 Dobbs 2000: § 317, 323, 329, Keeton, Dobbs, Keeton & Owen 1984: 376.

297 Beau Baez III 2014: 116. Referring to *Azzarello v. Black Bros. Co.* 480 Pa. 547 (1978) 391 A.2d 1020.

298 Dobbs 2000: § 353, Keeton, Dobbs, Keeton & Owen 1984: 681-689, Dommering-Van Rongen 2000: 19-30.

299 Beau Baez III 2014: 116.

300 Dobbs 2000: § 353, p. 977.

301 Watkins 2013: 660. Referring to Robert Moore, *Cybercrime, investigating high-technology computer crime* 6.

302 Watkins 2013: 660-661. Referring to Robert Moore, *Cybercrime, investigating high-technology computer crime* 6.

303 Lawyers talk of ‘click-wrap’ license, in analogy to ‘shrink-wrap license’ (discussed below).

the terms were presented in a sufficiently clear manner (conspicuous notice), a valid contract is formed.³⁰⁴

The law is less certain if the software has not been bought directly from the vendor, for example if the user bought a DVD with the software in a department store³⁰⁵ and installed the software from the DVD on his computer. Lawyers have debated whether a contract between the software vendor and the user comes about through a 'shrink-wrap license', being a license agreement that is arguably accepted by the user when opening the 'shrink-wrap' foil in which the software was packaged. In general, courts appear willing to accept that such shrink-wrap licenses are valid and lead to a contractual relationship³⁰⁶ on the condition that the terms are clearly readable and the person accepted them before buying the software.³⁰⁷ § 2.02 (b) of the Principles of Software Contracts use a 'reasonable person'-test for the validity of shrink-wrap licenses and similar formation processes.³⁰⁸ The practical relevance of this discussion is diminished as 'click-wrap' licenses, i.e. licenses which come about by clicking a button, are undoubtedly recognised by courts, and most software nowadays is either bought online (hence with a click-wrap license), requires acceptance of the license during installation, and/or requires additional acceptance of the license when installing updates. Vendors can ensure that a direct contractual relationship is established through the update process.

Here we will first discuss cases where a contractual relationship has been established. Then we will consider other legal grounds for action.

(1) *Contract*. In case of software the contract between vendor and user is usually called license agreement. License agreements for standard software are usually drawn up one-sidedly by the vendor.³⁰⁹ In such license agreements, the vendor or licensor generally excludes all important warranties and remedies, on a 'take it or leave it' basis.³¹⁰ Two exclusions concern us here: warranty disclaimers and limitations of liability and remedies.³¹¹

An explicit warranty provides a user with a ground for liability in case of breach of the warranty, but vendors usually refrain from formulating significant express warranties which

304 Hillman & O'Rourke 2010: 333. Referring to ALI Principles of Software Contracts, § 110-21.

Similarly Hillman & O'Rourke 2010: 1532, Moringiello & Reynolds 2010: 1551, Dickens 2007: 382 and 390.

305 Hence the contract of sale would be between user and store, not between user and vendor.

306 Blythe 2005: 91-92. Referring to ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), on which also Kuwahara 2007: 1018.

307 Blythe 2005: 91, referring to the analysis of Gringas 1996 regarding English law.

308 Moringiello & Reynolds 2010: 1549, Hillman & O'Rourke 2010: 1530. § 2.02(b) states "A transferee adopts a standard form as a contract when a reasonable transferor would believe the transferee intends to be bound to the form." It 'adopts the general contract-law objective test of contract formation'.

309 Rustad & Koenig 2005: 1553.

310 Rustad & Koenig 2005: 1562, cf. Carle & Perritt 2006: 47.

311 Scott 2008: 437.

would impose far-reaching duties on them. Hence a user would have to rely on implied warranties in case the software is found to be wanting. U.C.C. § 2-314 for example imposes an implied warranty of merchantability.³¹² Vendors may try to disclaim such implied warranties.³¹³ An example is the frequently used clause that the software is provided ‘as is’.³¹⁴ In general, implied warranty disclaimers are upheld by courts unless the disclaimers are unconscionable.³¹⁵ For example, U.C.C. allows sellers to disclaim warranties ‘as long as they are conspicuous’ (U.C.C. § 2-316(2)) and ‘to limit remedies on any undisclaimed warranties’ (U.C.C. § 2-719).³¹⁶ Similarly, UCITA § 406 allows the implied warranty of merchantability of computer programs to be disclaimed.³¹⁷

The ALI Principles of Software Contracts, on the other hand, recognise an implied warranty of no (material) hidden defects of which the software vendor³¹⁸ was aware at the time of the transfer (Principles of Software Contracts § 3.05) which cannot be excluded.³¹⁹ According to the comments, this simply restates accepted law.³²⁰ This provision implies that software may contain material defects, but these defects must be disclosed (i.e. must not remain hidden to the buyer).³²¹ However, if the defects are not even known to the vendor, there is – evidently – no duty to disclose. The net effect is that even if there might be a moral duty of diligence to avoid vulnerabilities in software,³²² there is no corresponding *legal* duty. Security defects in software (regardless as to whether they might have been avoided with more diligent development) do not constitute breach of contract, as long as the vendor is not himself aware of them, or if he is aware, discloses them.

If the vendor becomes aware of the defect at a later stage, there might be a duty to repair the defect within a reasonable time.³²³ In practice large vendors do patch vulnerabilities and make these patches freely available. This may be done in order to avoid liability for unclear disclosure of the defect, or be indicative of an actual duty to repair. One could see

312 See on the applicability of the U.C.C.: Kuwahara 2007: p. 1017 ff.

313 Scott 2008: 437-438, providing several reasons for disclaiming warranties. Referring to David Polin, ‘Proof of Manufacturer’s Liability for Defective Software’, 68 Am. Jur. Proof of Facts 3d. 333, 347 (2002).

314 Hillman & O’Rourke 2010: 1537.

315 Scott 2008: 438.

316 See further Kuwahara 2007: 1021 and Blythe 2005: 89, referring to U.C.C., § 2-719(3). The ALI Principles aim to replace the U.C.C. in this respect: Hillman & O’Rourke 2010: 1533.

317 Kuwahara 2007: 1021 footnote 164.

318 The Principles state ‘transferor’, in the present context we may simply refer to the software vendor.

319 Principles of the Law, The American Law Institute, Software contracts 2010: 193.

320 Principles of the Law, The American Law Institute, Software contracts 2010: 193, Hillman & O’Rourke 2010: 1534-1535, recognising that this is a controversial Principle.

321 Arguing the merits of the disclosure principle: Hillman & O’Rourke 2010: 1536-1537.

322 Pinkney 2002: 73 argues for a duty of due care, while recognising the necessity of a standard.

323 Cf. Dalsen 2009: 1089, arguing that slow response to a known vulnerability may amount to tortious negligence.

this as a remainder of a moral duty of diligence. Nonetheless, the original product need not conform to any standard of diligence.

The lack of a duty of diligence aside, a user would have few actual remedies if there would be a breach of warranty. The remedy of damages – which would usually be most applicable³²⁴ - is curtailed by the fact that the maximum amount of damages which is due for breach are, in practice, limited in the agreement.³²⁵ Such limitation clauses are generally valid,³²⁶ although for software the ALI Principles hold that damages may only be capped if the stipulated limit is reasonable in light of the anticipated or actual harm caused by the breach (§ 4.02).³²⁷ Even if the amount is reasonable, limitation clauses usually exclude compensation of pure economic loss. As cybercrime usually only leads to pure economic loss, such clauses effectively exclude any liability for damages.³²⁸

Hence, one can conclude that contract law does not provide significant remedies against software vendors who do not exercise the desired diligence in the prevention of foreseeable cybercrimes.³²⁹

(2) *Product liability.* A frequently discussed alternative is to apply product liability to software.³³⁰ The law as it stands at present does not allow this. The Third Restatement itself does not specify clearly whether software is a service or a product.³³¹ However, when applying product liability law courts generally consider software to not be a product,³³² since a product has to be tangible.³³³

Furthermore, even if product liability law would apply to insecure software, this would not improve matters. Firstly, product liability does not lead to recovery of pure economic

324 The remedy of specific performance consisting of correcting the defect is not invoked in practice, as companies voluntarily provide patches (see above).

325 Rustad and Koenig 2005: 1558-1559.

326 Guarino 2002: 583, Scott 2008: 440. Referring to *Caudill Seed & Warehouse Co. v. Prophet 21, Inc.*, 123 F. Supp. 2d 826, 829 (E.D. Pa. 2000).

327 Principles of the Law, The American Law Institute, Software contracts 2010: 261. This is based on U.C.C. § 2-718, UCITA 804 and Second Restatement § 356(1). Compare also U.C.C. § 2-719 (3).

328 Kuwahara 2007: 102 therefore concludes that the victim may not be able to demonstrate any recoverable damage.

329 Cf. Rustad & Koenig 2005: 1566, Carle & Perritt 2006: 47, also Chong 2013d.

330 Cf. Alces 1999.

331 Childers 2008: 144. Referring to Second Restatement § 402A and Third Restatement § 19. Dobbs 2000: § 376 (still) does not discuss software.

332 Childers 2008: 128 and 142, with references, cf. Scott 2008: 462, also Rustad & Koenig 2005: 1577, pointing out that no court has considered software to be a product under Third Restatement § 19. Weber 1992 argues that software is a product under § 402A.

333 Childers 2008: 146. Referring to Third Restatement § 19a. See also the detailed discussion in Lannetti 2000.

loss.³³⁴ Even though it has been argued that some claims based on unsecure software should be recoverable despite the economic loss rule,³³⁵ this has not been accepted as law. Secondly, in case of commercial relations (i.e. where the user is a business), courts have generally found that the U.C.C. allows limitation clauses for product liability claims based on damage to property.³³⁶ Hence these rules would also need to be modified if product liability for software is to provide effective incentives.³³⁷

There is nonetheless academic support for applying product liability law to software, possibly by extending the current definitions.³³⁸ In particular, it is argued that mass-market software should be qualified as a product.³³⁹ Alternatives to strict product liability for (embedded) software have been suggested, such as the common tort of negligence (see below),³⁴⁰ implied product warranties (discussed above), professional malpractice of software developers (see s. 8.3), hardware based product liability, and misrepresentation.³⁴¹

(3) *Tort of negligence.* If neither contractual liability nor product liability provides grounds for a claim, the tort of negligence might apply.³⁴² This presumes that no contractual relationship has been established, otherwise there usually will be a limitation clause (see above) which would prohibit an award of damages even if negligence can be established. As discussed above, there may be cases in which there is no actual contract between vendor and user (such as in the case of free software). Furthermore, there is the issue of third party liability, i.e. if a third party suffers losses because of a vulnerability in the software provided by the vendor and used by the user. An example might be a DDoS attack made possible by an infection of the user through a vulnerability in standard software: the

334 Scott 2008: 470 calls this 'the most significant impediment' to application of product liability law to software. See also Kuwahara 2007: 1012, Gripman 1997: 177. Referring to *People Express Airlines v. Consolidated Rail Corp.* 100 N.J. 246, 495 A.2d 107 (1985). *J'Aire Corp v. Gregory*, S.F. No. 23983, August 13, 1979. 'But see' *Dundee Cement Co v. Chemical Labs.* 712 F.2d 1166, No. 82-2894 (7th Cir. 1983).

335 Scott 2008: 471. Referring to *Spagnol Enters., Inc. v. Digital Equip. Corp.*, 568 A.2d 948, 951–52 (Pa. Super. Ct. 1989).

336 Scott 2008: 471.

337 A further discussion of whether extension of product liability to embedded software (which is different from the standard software discussed here) is appropriate can be found in Childers 2008: 152-175.

338 Brenner 2004a and 2004b, Childers 2008: 128 and 146, referring to Bonna Lynn Horovitz, 'Computer Software as a Good under the Uniform Commercial Code: Taking a Byte Out of the Intangibility Myth', 65 B.U. L. Rev. 129, 151-52, Proof of Facts par. 4 at 333 n.2., David Polin's, 'Proof of Manufacturer's Liability for defective software' 2005, David W. Lanetti, 'Toward A Revised Definition Of "Product" Under The Restatement (Third) of Torts: Products Liability', *Tort & Ins. L.J.* 845 (1999-2000): 845-890.

339 Childers 2008: 141. Referring to Third Restatement § 19 cmt. d.

340 Childers 2008: 141. Referring to Third Restatement § 19 cmt. a (1998).

341 Childers 2008: 175-182.

342 See on the applicability of negligence law: Rustad & Koenig 2005 p. 1586 ff. (who argue for a new tort of negligence enablement of cybercrime, p. 1571), Scott 2008: 442.

business suffering the attack would be such a third party.³⁴³

Under common law negligence rules it is highly unlikely that a software vendor would be found liable for providing software with vulnerabilities.³⁴⁴

First of all, negligence requires the existence of a duty of care³⁴⁵ and a subsequent breach of that duty. One could argue that there would be two duties of the vendor: 'a duty to design and develop secure software' and 'a duty to instruct the licensee on how to use its products safely and to warn them of hidden dangers that the products may contain'.³⁴⁶ Because vendors 'are the only one who can isolate and repair the problems', it has been argued that 'software vendors owe a duty to their licensees and to society as a whole to ensure the security of their software'.³⁴⁷ However, it is quite uncertain whether courts would actually find that such a duty exists.³⁴⁸

Even if this duty exists, there would be considerable problems in determining an appropriate standard of care.³⁴⁹ There are no generally accepted standards as to when a vendor would breach a duty to provide secure software,³⁵⁰ even though several authors propose such a standard.³⁵¹

A second obstacle is the fact that cybercrimes usually involve only non-physical losses, such as loss of data, financial harm, dignitary injury and the invasion of privacy. These fall under the heading of pure economic loss. An action on the basis of negligence, according to the law in most states, cannot as a rule lead to recovery of pure economic loss.³⁵² This would effectively preclude an award of damages in the case of negligence based on insecure software,³⁵³ unless the courts make an exception in case of public policy reasons.³⁵⁴ An award of punitive damages would be possible only if aggravated circumstances, such as

343 There is a complicated question what happens if the business also uses the standard software. In all probability the license agreement would also contain a liquidated damages clause for such a case.

344 Weber 1992: 478, Levy & Bell 1990.

345 On which Cardi & Green 2008.

346 Scott 2008: 443. Referring to Owen, Products liability law, § 2.1, at 62–63.

347 Scott 2008: 444. Referring to Brooks, Jr, The Mythical man-month: essays on software engineering, at 183–84.

348 See the pro-liability argument by Scott 2008: 443, who still recognises the significant uncertainty for this question. Referring to John L. Diamond et al, Understanding torts § 8.01, at 118 (2d ed. 2000) Michael L. Rustad, The Negligent Enablement of Trade Secret Misappropriation, 22 Santa Clara Computer & High Tech Law Journal 455: 519–20 (2006), based upon factors set forth in Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968). Asserting that existing law does not recognise such a duty: Rustad & Koenig 2005: 1603nt15, cf. Finch & Spiegel 2014: 363.

349 Scott 2008: 444–448.

350 Scott 2008: 448. See also the discussion in s. 4.4.3 above.

351 Scott 2008: 448, referring as an example to Rustad & Koenig 2005.

352 E.g. Bernstein 1998. Scott 2008: 453 holds that current case law is divergent on this issue.

353 Carle & Perritt 2006: 47.

354 Kuwahara 2007: 1025.

intent or reckless behaviour) can be proven.³⁵⁵

It should be noted, however, that the California Supreme Court has ruled that pure economic loss may in particular circumstances be recovered on the basis of negligence, subject to the restrictions of foreseeability and proximate cause.³⁵⁶ This exception, however, is limited to the case in which there is a special relationship between the defendant and the claimant. Furthermore, recovery of pure economic loss on the basis of negligence is not possible if there is a contractual relationship between parties.³⁵⁷ Hence this exception to the economic loss rule would not help in case of software.

We can conclude that at present there is no action in tort for the production of software which enables security breaches and foreseeable cybercrime.³⁵⁸ This would only be different in case of reckless disregard of the probability that the plaintiff would be harmed.³⁵⁹

There are several academic articles pleading for a change in the law.³⁶⁰ An example is the proposal to introduce a duty of care to develop safe software.³⁶¹ In support of an argument for tort liability, it has been argued that software vendors who do not fix a known security flaw may be the proximate cause of a security breach.³⁶²

(4) *Gratuitously provided software*. Finally, a few remarks as to the legal status of software which is provided for free. In general, one can distinguish between open source software and freeware. Open source software is generally provided for free, but with a license binding the user to specific actions and restrictions,³⁶³ including limitations of liability. Although there is no monetary consideration, consideration can be found in promises, acts or forbearances. In the case of *Jacobsen v. Katzer*³⁶⁴ the U.S. Court of Appeals for the Federal Circuit held that, for the specific open source license involved in

355 Meurkens 2014: 61.

356 SCOCAL, *J'Aire Corp. v. Gregory*, 24 Cal.3d 799, S.F. No. 23983, August 13, 1979. Available at: (<http://scocal.stanford.edu/opinion/jaire-corp-v-gregory-30547>) (last visited Friday February 6, 2015): "(...) recovery for negligent interference with prospective economic advantage will be limited to in-stances where the risk of harm is foreseeable and is closely connected with the defendant's conduct, where damages are not wholly speculative and the injury is not part of the plaintiff's ordinary business risk"

357 *Aas v. Superior Court (William Lyon Company)* (2000) 24 Cal.4th 627 , 101 Cal.Rptr.2d 718; 12 P.3d 1125.

358 Rustad & Koenig 2005: 1557. Incidentally, in specific cases involving anti-terrorism software, the SAFETY act may lead to immunity for liability. See Finch & Spiegel 2014: 368 for details.

359 As is the criterion used for finding ground for awarding punitive damages.

360 Dalsen 2009, Rustad & Koenig 2005. See also Finch & Spiegel 2014.

361 Rustad & Koenig 2005: 1558. Referring to Robert L. Rabin, 'Enabling Torts', *Deapul Law Review* 1999, 435, 452.

362 Dalsen 2009: 1088.

363 Particularly having to do with providing source code for free, being obliged to make publicly available all modifications and improvements to the software ('viral effect'). See generally Rosen 2005.

364 535 F.3d 1373 (Fed. Cir. 2008).

the case, a number of requirements, such as the requirement to give credit to the original author, constituted sufficient consideration.³⁶⁵ Similarly, the use of the software may be considered acceptance of the license, thereby completing a contract. Assuming that most open source licenses are, in the relevant aspects, similar to the license involved in this case, the conclusion is that the use of open source software will generally establish a contractual relationship.³⁶⁶ We already provided a contractual analysis of software liability above.

Software may also be provided for free in a situation different from the open source license. The significant difference between those two cases is that the vendor of open source software requires the user to adhere to certain rules and restrictions, while the maker does not require any particular action by the user for other types of free software: he is simply happy if the software proves useful to other people. It is therefore less clear that a contractual relationship exists, as on the one hand there is no clear consideration, and on the other hand it may be open to doubt whether mere use of the software is sufficient to assume acceptance. It may even be doubted whether the document provided with the software constitutes an offer to conclude a contract.³⁶⁷ Assuming that no contract is established, the user could only have an action on the basis of tort, in particular the tort of negligence. Such an action would usually not lead to liability. First of all, the developer of the software would not be held to a high standard of care, as he would usually stipulate in the license that he does not provide any warranty that the software is free of defects. Secondly, any warning that the user uses the software at his own risk would stand in the way of a successful action, as the court would find that by consenting to the risk of defects, the user has taken on the responsibility, whereby no duty of care exists or no breach of duty can be assumed.³⁶⁸ Finally, the economic loss rule discussed above would apply here as well.

5.3.2.4. ISPs

As ISPs have a central position in Internet communication, there has been considerable discussion as to whether they should become more active or, on the contrary, should remain neutral. Corresponding liability regimes have been discussed. There is vocal opposition to the current lack of accountability ISPs,³⁶⁹ but also support for non-liability for mere transfer of data.³⁷⁰ It has been argued that ISPs have a regulatory function and can

365 Cf. Earl 2009: 1619, more general Hillman & O'Rourke 2009.

366 Hillman & O'Rourke 2009, Hillman & O'Rourke 2010: 1523.

367 This would depend on the actual phrasing. Such documents are usually called license or disclaimer.

368 See Dobbs 2000, § 213-214 and § 211 on the earlier doctrine of assumed risk, also Sergienko 2006.

369 Lichtman 2004-2005: 54, Peterson, Segal, Eonas 2014: 587 and 596. Referring to Mann & Belzley 2005 and N. Shachtman, Brooking Inst., *Pirates of the ISPs: Tactics for turning online crooks into international pariahs* 3 (2011). Also De Villiers 2005: 17.

370 Harper 2005: 31.

monitor and control cybercrime, even though they have as of yet avoided liability.³⁷¹

The legal landscape is complicated by several specific statutory provisions. With regard to the current topic we may pass over some details.

In the first place, ISPs may enjoy immunity for copyright infringement on the basis of the Digital Millennium Copyright Act (DMCA). ISPs are not liable if they are merely passive networks,³⁷² provided they have no knowledge of the infringement.³⁷³ They only incur liability when they have received notice of the alleged infringing material and have not made the material inaccessible.³⁷⁴ These rules have been criticised: '[c]ourts interpreting these provisions have reinforced this apparent trend away from ISP liability by, among other things, interpreting these statutes to preempt state laws that would otherwise have encouraged ISPs to take due care'.³⁷⁵

Secondly, regarding the hosting, making available or transmittance of obscene or otherwise objectionable material,³⁷⁶ ISPs again enjoy an immunity for material not originating from the ISP itself.³⁷⁷ It is noteworthy that, in contrast to EU rules, the ISP may under par. 230 of the Communications Decency Act also take positive actions to filter such unlawful material without thereby losing its immunity. This rule was enacted to counteract an earlier precedent whereby an ISP lost its immunity by trying to remove wrongful material.³⁷⁸ The legislator considered such a rule to be counterproductive as it provided a strong disincentive to take socially desirable efforts to remove wrongful materials. This rule has also been criticised: although it removes the 'chilling effect' of potential liability, it does not incentivise ISPs to monitor content.³⁷⁹

Thirdly, the common rules of negligence apply to other cases, but the categorisations used for the making available of information are taken into account. Whether ISPs are liable

371 Peterson, Segal, Eonas 2014: 597. Referring to Lichtman & Posner 2004.

372 Watkins 2013: 659. Referring to Lori E. Lesser, Current Copyright Internet Litigation Issues, 932 PLI/Pat 349, 359 (2008). Also Lichtman & Posner 2006: 223, Lichtman & Posner 2004: 4. Referring to 17 U.S.C. §512(a). Furthermore Amadei 2001: 214. Referring to 17 U.S.C. 512 (a) (network communications), (b) (access), (c) (data stored) and (d) (providing information locations tools).

373 Lichtman & Posner 2006: 223, Lichtman & Posner 2004: 4. Referring to 17 U.S.C. §512(c)-(d).

374 The practice of acting correctly in this manner to avoid liability is referred to as a Notice and Take Down procedure.

375 Lichtman & Posner 2006: 223. Lichtman & Posner 2004: 4.

376 Fully 'obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable': Amadei 2001: 213. Referring to 47 U.S.C. § 230 (c) (2) (1996).

377 Lichtman & Posner 2006: 222-223, Lichtman & Posner 2004: 3-4, Materna 2012: 130.

378 *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995): the court found that the bulletin board (a precursor of a hosting ISP) took editorial actions and therefore became a publisher.

379 DLA Piper 2009: 33.

is dependent on their classification as carriers, publishers or distributors.³⁸⁰ The mens rea element is critical in case of the carrier classification. To a publisher 'would attach a high degree of culpability'. A distributor is less likely to face liability than a publisher.³⁸¹ Regardless of the precise classification of an ISP, there is little possibility of a successful claim in case of content that leads to cybercrime, as can be shown by an analysis of the requirements and possibility of an action on the basis of negligence.

Carle and Perritt have discussed the different requirements for a claim of negligence against an ISP. For such a claim to be successful, the plaintiff has to tackle several obstacles and prove a number of requirements. Firstly, he has to prove that the ISP owes a duty of care to the consumer. Secondly, he has to prove the appropriate standard of care,³⁸² and, thirdly, that this standard is not met, amounting to a breach of duty. Furthermore, the ISP has had to cause injury. The plaintiff has to prove personal injury or damaged property and that the injury was preventable and foreseeable.³⁸³ Hence, similar to the discussion on negligence of software vendors (s. 5.3.3.1), a negligence action has little chance of success.

Many authors argue for the introduction of indirect liability of ISPs. Peterson, Segal and Eonas note 'the better position of ISPs', arguing that ISPs 'are better able to internalize negative externalities'. It would be appropriate to recognize indirect liability of ISPs because of their position, allowing them to detect activities and internalize negative externalities.³⁸⁴ Lichtman and Posner think that indirect liability is attractive because 'ISPs are in a good position to deter the various acts associated with cyber-insecurity'. Moreover, 'liability would force ISPs to internalize some of the negative externalities they impose'. Indirect liability should be incorporated in law instead of contract. Many of the actors are 'beyond the reach of the law' and transaction costs could be an obstacle to contractual solutions.³⁸⁵ Service provider liability is attractive because 'ISPs are in a good position to reduce the number and severity of bad actors online' and because 'intuition finds support even within the aforementioned immunity and safe harbor statutes'.³⁸⁶

In conclusion, despite the recognition of the central position of ISPs, there is as yet no duty of care and diligence to take positive action to protect against cybercrime.

380 Peterson, Segal, Eonas 2014: 602. Referring to Mark Tatum, 'Internet Crimes: Legal Responsibility of Internet Service Providers', *Computer L. & Sec. Rep.* 1998, 383, 383-86. Also Amadei 2001.

381 Peterson, Segal, Eonas 2014: 602. Referring to *ibid*, 384.

382 Carle & Perritt 2006: 46.

383 Carle & Perritt 2006: 47.

384 Peterson, Segal, Eonas 2014: 598, Materna 2012.

385 Lichtman & Posner 2006: 240, Lichtman & Posner 2004: 22-23, Lichtman 2004-2005: 58.

386 Lichtman & Posner 2006: 223, Lichtman & Posner 2004: 4.

5.3.2.5. *Businesses*

Businesses may have two kinds of duties of care and diligence which are relevant here:

- diligence to ensure the availability of the services provided, and
- care and diligence to avoid security breaches leading to a loss of private data.

The interest protected by the first duty of diligence is imperilled by DDoS attacks. The interest involved in the second duty is imperilled by ransomware, and also by other kinds of security breaches possibly, but not necessarily, involving malware. As security breaches are an important attack vector for malware, we will discuss the more general topic of duties of care and diligence against security breaches.

(1) If a business has a duty towards its customers to ensure the availability of its services, this encompasses a duty to take appropriate measures against DDoS attacks. But do businesses have such a duty? It is regularly presumed that there is a moral duty to try to take sufficient measures. However, legally speaking the contract determines to what extent a business is actually obliged to do more. Business contracts commonly limit the obligations regarding the availability of services, as it is impossible to unconditionally guarantee 100% service availability. Hence any warranty regarding availability is probably limited to such an extent that even more extensive outage because of a DDoS-attack would not be a breach of contract. An implied warranty would not be more extensive given the present impossibility to ensure availability. Arguably, this might be different if a DDoS-attack is of extensive duration (more than several days), but at present this is rare. Furthermore, given the current state of technology, DDoS attacks are hard to counter effectively; hence such an attack might count as *force majeure*, offering an excuse of the breach. One would expect businesses to draft their contracts in such a way that DDoS attacks do fall under *force majeure*.

Arguably, a businesses might also be under an obligation of best effort to prevent and combat DDoS attacks. However, given the lack of clear standards to prevent such attacks, it appears unfeasible to prove a lack of effort, except in extreme cases of negligence.

Finally, a claim of damages would usually fail as the losses involved would generally be classified as pure economic loss, a category which is generally not recoverable.

Hence, insofar as a legal duty of diligence is recognised, it usually cannot be enforced effectively - except if the business did not follow common contract practices or was exceedingly negligent in taking appropriate measures.

(2) A number of rules apply to security breaches that lead to infection and/or to exposure of private data.³⁸⁷

First of all, a claim for negligence might exist if a business network is infected and used as a basis of a DDoS attack. Another business suffering from the DDoS attack could

³⁸⁷ Cf. the broad analysis of Sulkowski 2007.

claim negligence as the other business should have secured its network sufficiently.³⁸⁸

Perhaps most important are the rules imposing security breach notifications. These rules are effectively duties of administrative law (see s. 5.3.4). They imply a duty of care or diligence towards the customers of the norm addressee to take sufficient security measures to prevent a security breach, even though the primary cause of the breach is the criminal himself.³⁸⁹ Such a duty could be viewed as a non-excludable implicit warranty that sufficient security measures will be taken, or as a non-excludable obligation of best effort towards security. Regardless of the precise legal ground, this leaves open the question which standard is to be applied for determining the measures that are to be taken.³⁹⁰ At present there are no generally accepted standards.³⁹¹

There is discussion as to whether the loss of private data may lead to recoverable damages, notwithstanding the economic loss rule. Private individuals may be able to start an action on the basis of tort law. It is argued that tort law would allow the most flexible and adaptable standard to be applied.³⁹² However, a recent analysis argues that there is hardly any legal recourse available to consumers after a security breach.³⁹³

5.3.3. *Criminal law*

Criminal law – federal and state law - has been modified substantially in order to allow the prosecution of cybercrime.³⁹⁴ The U.S. acceded to the Cybercrime Convention in 2006 (see s. 7.3). The relevant forms of cybercrime discussed therein are all punishable.³⁹⁵

Exploitation by ransomware is a federal offense, as 18 U.S.C. § 1030(a)(7)³⁹⁶ declares punishable whomever, “with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any (A)

388 Sulkowski 2007: 59, drawing the analogy with leaving car keys in the ignition (leading to joy-riding), which has been found to be negligent on the part of the car owner (referring to *Abdallah v. Caribbean Sec. Agency*, 557 F.2d 61, 63 (3d Cir. 1977); *Vining v. Avis Rent-A-Car* 354 So. 2d 54, 55 (Fla. 1977)). Also arguing for tort liability: Sinrod & Reilly 2000: 203.

389 Cf. Sulkowski 2007: 62, speaking of a ‘common-sense responsibility’.

390 Cronin 2010.

391 Shaw 2010: 557-559 proposes adopting the PCI-DSS standard from the payment card industry as a safe harbor. Peters 2014: 1196 also argues for a better defined standard or best practice, with a regulatory agency that keeps the standard up to date (also p. 1198).

392 Sulkowski 2007: 61, 47-49 (partly not about privacy, but regarding a claim by another business).

393 Peters 2014. She proposes, among others, an additional private cause of action (p. 1197).

394 See primarily the overviews of Mehra 2010 (who focuses mainly on IP infringement and child pornography) and Kim c.s. 2012, and earlier Sinrod & Reilly 2000, Burstein 2003.

395 See also the analysis by Sulkowski 2007: 25-30. As regards penalties, see Kim c.s. 2012: 463-464. For state legislation see Kim c.s. 2012: 481-484.

396 18 U.S.C. § 1030 is often referred to as the Computer Fraud and Abuse Act (CFAA).

threat to cause damage to a protected computer;³⁹⁷ (...), (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion”.

DDoS attacks may be prosecuted as causing intentional damage to a protected computer by the transmission of information or of a command (18 U.S.C. § 1030(a)(5)(A)).³⁹⁸ Renting out a botnet for DDoS attacks is evidently also an offense.³⁹⁹

Violations of 18 U.S.C. § 1030 may also be investigated by the U.S. Secret Service.⁴⁰⁰ Private individuals harmed by offenses under 18 U.S.C. § 1030 may claim damages in a civil action.⁴⁰¹

The cybercrime provisions of the California Penal Code are modelled on the Federal CFAA. Title 13, Chapter 5, § 502(c) covers the relevant forms of cybercrime by declaring punishable actions such as the use of computers or networks to extort, use and access computer services or data without authorization, causing denial of computer services.⁴⁰² Title 13, Chapter 5, § 502(c)(5) declares punishable whomever “[k]nowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network”.⁴⁰³ Title 13, Chapter 5, § 502(c)(8) declares punishable whomever “[k]nowingly introduces any computer contaminant into any computer, computer system, or computer network”. These provisions cover ransomware and DDoS attacks.

In comparison to the Federal CFAA, these provisions have a lower threshold of knowledge, as mere knowledge rather than intent is required.⁴⁰⁴

As these provisions show, the focus of criminal law regarding cybercrime is on punishing the principal offenders. Contributory actors only come into play insofar as they can be considered accessories. Accessory liability for federal crimes is based on 18 U.S.

397 protected computer means (besides government computers) a computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States”: 18 U.S.C. § 1030(e)(2)(B)

398 Carroll 2003. See for an example <http://www.justice.gov/usao-ndca/pr/thirteen-defendants-plead-guilty-december-2010-cyber-attack-against-paypal> and the original indictment on <https://docs.google.com/file/d/oBzqf52Yc4ogyDNGbXEXHFtQoU/edit?pli=1> See also about the criminal liability for DDoS attacks: McLaurin 2011: 222-231.

399 See *U.S. vs. Ancheta*, 06-051 (C.D. Cal.), Febr. 2005 Grand Jury, available at <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>.

400 18 U.S.C. § 1030(d)(1).

401 18 U.S.C. § 1030(g).

402 The actual provisions are of course much more detailed and extensive.

403 See <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9>.

404 Carroll 2003.

Code § 2(a).⁴⁰⁵ Also punishable is the accessory after the fact.⁴⁰⁶

In theory, ISPs might be accessory to cybercrime, as they are closely involved with the Internet communication that makes cybercrime possible, and furthermore have much data available and could actively take steps to prevent cybercrime. The immunity of Communications Decency Act § 230 does not apply to criminal liability.⁴⁰⁷ However, the criterion of ‘aiding and abetting’ is to be presumed to set a sufficiently high barrier that an ISP acting in good faith should not be considered an accessory. Mere negligence that facilitates a crime is not sufficient; to be convicted of aiding and abetting, an accomplice must have the requisite *mens rea*, which requires knowledge that every element of the crime is intended.⁴⁰⁸ This amounts to a requirement of *intent*.

For similar reasons, a software vendor may not be held liable merely for leaving vulnerabilities in software, particularly if he is not aware of the vulnerability. The software vendor would lack intent for the crimes committed through abuse of the vulnerability, except in cases of gross negligence bordering on intent. The same reasoning applies to a business who through lack of effort becomes the victim of cybercrime, even where this affects others (for example because the business computers become part of a botnet).

5.3.4. Administrative law

A particular feature of US law, adopted by other legal systems later on, is the existence of security breach notification laws.⁴⁰⁹ The reason for enacting such laws was that companies regularly started becoming the victim of security breaches by which unauthorised third parties could access personal data. Notification laws obligate companies to notify public authorities (and sometimes also the individuals whose data was compromised) of such a

405 “Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.”

406 18 U.S. Code § 3: “Whoever, knowing that an offense against the United States has been committed, receives, relieves, comforts or assists the offender in order to hinder or prevent his apprehension, trial or punishment, is an accessory after the fact.
Except as otherwise expressly provided by any Act of Congress, an accessory after the fact shall be imprisoned not more than one-half the maximum term of imprisonment or (notwithstanding section 3571) fined not more than one-half the maximum fine prescribed for the punishment of the principal, or both; or if the principal is punishable by life imprisonment or death, the accessory shall be imprisoned not more than 15 years.”

407 Section 230(e)(1) Communications Decency Act.

408 See *Rosemond v United States*, case no. 12-895, decided 5 March 2014, available at http://www.supremecourt.gov/opinions/13pdf/12-895_3d9g.pdf. This applies to federal crimes, but presumably this will also be followed for state crimes, as the Supreme Court interpretation of federal accessory liability will presumably be leading for interpretation of the analogous parts of the Model Penal Code which is mostly followed by state courts.

409 See for the following Schwartz & Janger 2007, Winn 2009, Shaw 2010, Rode 2007.

breach. The first law of this kind was the California data security breach notification law of 2002.⁴¹⁰

Notification laws currently apply to specific industries,⁴¹¹ while more general laws exist at the state level.⁴¹² The laws differ as to the details of what the notification entails and who has to be notified.⁴¹³ On 12 January 2015, the White House proposed a Personal Data Notification & Protection Act.⁴¹⁴ Although notification laws only require companies to notify authorities and do not connect any negative consequences to the notification itself, the existence of such laws has had positive effects on the prevention of security breaches.⁴¹⁵ A further consequence is the rise of cybersecurity insurance, which has led to improved security measures (s. 6.6.2). Furthermore, specific statutes allow consumers to collect damages in case of untimely notification.⁴¹⁶

The FCC (see s. 6.3.3) may promulgate rules applicable to ISPs.⁴¹⁷ FCC rules are found in Title 47 of the Code of Federal Regulations (CFR). Under the FCC Open Internet Order 2010, a number of rules were added to section 8 of Title 47.⁴¹⁸ Presently the focus is on transparency rather than specific standards, as evidenced by § 8.3 Title 47 CFR. This provision does not impose mandatory standards, but rather requires ISPs to disclose how they operate with respect to “network management practices, performance, and commercial terms” of service.⁴¹⁹ The FCC has recently adopted new rules,⁴²⁰ which adopt the principle of net neutrality (see also s. 7.4).

There are several constitutional issues with cybercrime. Of particular importance is

⁴¹⁰ S.B. 1386, 2001-2002 Leg., codified at Cal. Civ. Code § 1798.29 and § 1798.80-84.

⁴¹¹ For health care see the Health Insurance Portability and Accountability Act 1996 (HIPAA) Breach Notification Rule, 45 CFR §§ 164.400-414 (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breach-notificationrule/>). See further the exam-ples in Shaw 2010: 534-542, Rode 2007: 1613-1619.

⁴¹² See the list at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>. For California see Cal. Civ. Code §§ 1798.29, 1798.80 et seq. An examination of differences can be found in Shaw 2010.

⁴¹³ Critical about the diversity in laws: Joerling 2010.

⁴¹⁴ <http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families>, see <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf>

⁴¹⁵ Rode 2007, and Schwartz & Janger 2007: 913, referring to Sunstein 1999: 613 as to the more general trend in US legislation of ‘regulation through disclosure’, who further refers to earlier articles of, among others, Stephen Breyer and Anthony Ogus.

⁴¹⁶ Shaw 2010: 529.

⁴¹⁷ It should be noted that it is debated to what extent the FCC does have jurisdiction: see Scala 2011, Sherling 2014.

⁴¹⁸ https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.

⁴¹⁹ This rule was upheld in *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014), while § 8.5 (disallowing blocking of lawful content) and § 8.7 (forbidding unreasonable discrimination) were vacated.

⁴²⁰ On 26 February 2015: <http://www.fcc.gov/document/fcc-adopts-strong-sustainable-rules-protect-open-internet>.

the Fourth Amendment to the Constitution, protecting privacy. It has, for example, been interpreted by the Supreme Court as prohibiting the large-scale collection of data.⁴²¹ See further on this topic section 7.4.

5.3.5. *Conclusion*

U.S. law provides limited recognition of duties of care and diligence. With respect contract law, the primary actors (ISPs, software vendors and businesses) considered here would have to be held liable on the basis of warranties. However, contracts are usually drafted to avoid extensive warranties, and this is generally accepted with only few limitations. In particular for the kind of cases here limited warranties would be acceptable. Furthermore, even if a breach of warranty would be found, limitation clauses would have the effect that hardly any damages would have to be paid. Only for businesses there may be a possibility of being held liable, in particular in case of a security breach leading to loss of personal data. With respect to tort law, ISPs are mostly immune for liability given specific laws and the general rules for negligence. Software vendors and businesses would not be held liable for negligence, or at least would not have to pay damages as the loss would mostly involve pure economic loss, which is as a rule not recoverable under U.S. law. Criminal law does recognise the possibility of aiding and abetting cybercrime, but this requires intent. Contributory actors acting negligent but in good faith would not fulfill this requirement. Administrative law provides few rules to govern ISP behaviour, although there are currently some initiatives, such as a proposal for adopting the principle of net neutrality. Noteworthy is the widespread acceptance of notification duties.

5.4. *Brazil*

The principle of duty of care as a requirement for caution and scrutiny relates to the notion of due diligence, which can be found in Roman law. In this regard, the influence of traditional Roman law has also reached Brazil because of the adoption of a civil law system. Today, elements of care and diligent behaviour can be found in different areas of the national framework. For the purpose of this report, we look at how the requirement of care and diligence has been transposed to private (contract, tort and consumer law) and public law (criminal and administrative law) and how an overall requirement for care and diligence can be used to understand the liability of business, ISPs and software developers in relation to security incidents.

5.4.1. *Civil law*

The Brazilian legal system follows the civil law tradition because of Brazil's colonization

421 United States v. Jones, 132 S. Ct. 945 (2012), as interpreted by Gray & Rinehart 2013.

process. Brazilian civil law is composed of a codified set of laws which follows the general principles laid down in the Federal Constitution, specified at the federal level by the Brazilian Civil Code (BrCC). Although enacted in 2002, the current Brazilian Civil Code was largely drafted in the 1970s and largely inspired by the German, Italian and Portuguese civil codes.⁴²² It goes without saying that by the time the code entered into force, many of its provisions no longer provided the much needed and expected modernization of Brazilian civil law.

Nevertheless, the Brazilian Civil Code of 2002 introduced important changes to the Brazilian legal system by incorporating elements which case law and specific statutes later reinforced. Because of the Consumer Protection Code of 1990, a large portion of contract law that was covered by the old Civil Code of 1916 is then regulated as part of consumer relations. The Brazilian Civil Code of 2002 therefore regulates a narrower set of situations than its predecessor, as its applicability is limited by consumer law.⁴²³ Furthermore, whilst the Brazilian Civil Code dedicated a special title to torts, several tort provisions spread throughout the code continue to coexist.⁴²⁴ Moreover, tort provisions can also be found in the Consumer Protection Code and even the Federal Constitution, regarding, for instance, State Liability.⁴²⁵

5.4.1.1. *Contractual torts*

Brazilian civil law was largely influenced by the classic Roman legal tradition, with the addition of several principles of German civil law and alike provisions. Generally speaking, contracts as bilateral or multilateral consensual agreements established with the purpose of creating legal effects between the parties.⁴²⁶ In 2002, the legislator introduced important principles of public law into the Civil Code in an effort to align private law with constitutional rights. This resulted in the introduction of principles of social function (Art. 421 BrCC), good faith (Art. 422 BrCC) and supremacy of public order (Art. 2035 BrCC).⁴²⁷ Moreover, both parties must act with diligence as they are under a duty to prudently and carefully examine the object of the contract and its characteristics.⁴²⁸ Caution and diligence are mostly preventive duties,⁴²⁹ in the sense that they must be exercised before conclusion of

⁴²² Tomasevicius Filho 2013: 211-221: 216.

⁴²³ The Consumer Protection Code covers different areas of law, including criminal law, procedural law and administrative law.

⁴²⁴ Cavalieri Filho 2003: 31-47: 44.

⁴²⁵ See art. 37, §6ffl of the Brazilian Federal Constitution.

⁴²⁶ da Silva Pereira 2013: 59.

⁴²⁷ Pasqualotto 2002 : 219-235 : 219.

⁴²⁸ Tepedino 2012: 30.

⁴²⁹ Tepedino 2012: 31.

the contract, but they remain present throughout the entire contractual relation as a rule of conduct and behaviour. However, such a duty to act prudently, carefully and with diligence is not clearly provided for by the BrCC.

The Brazilian Civil Code regulates several forms of contracts (*contratos típicos*). It gives parties the possibility to create sui generis rules for non-regulated contracts (*contratos atípicos*), which must nevertheless obey the general principles and validity requirements prescribed by the Civil Code and be interpreted in line with the ratio of the closest *contrato típico*. In Brazilian contractual hermeneutics, *Willenstheorie* prevails over the *Erklärungstheorie*.⁴³⁰ Art. 112 BrCC determines that in declarations of will, the shared intention shall prevail over strict literal meaning of the declaration. Art. 113 BrCC complements the set of interpretation rules by establishing that legal transactions shall be interpreted according to the good faith and custom of the place of making. Therefore, the common intentions of the parties and the customs of the place where the contract is concluded are important elements of contractual interpretation in Brazilian law.

The general theory of obligations was drafted in accordance with the German dualistic tradition. Once the contractual obligation is fulfilled, debt (*Schuld*) and liability (*Haftung*)⁴³¹ are exhausted. However, if one of the parties foregoes his obligation, the party that did not give cause to the breach (creditor) may request termination of the contract by claiming “exceptio non adimpleti contractus” (Art. 476 BrCC) so as to sustain the reciprocity of his own obligation. But the “exceptio non adimpleti contractus” may not provide relief in all situations, especially if the debtor has already received its portion of the contract.⁴³² In this case, the creditor may be entitled to demand the situation to be restored to the status quo ante.⁴³³ It goes without saying that returning to the status quo ante (i.e. the conditions that existed prior to the breach or to the contract itself) is often an impossible task. Therefore, in contractual law re-establishing the status quo ante is understood as providing the creditor with material compensation that will satisfy the party in a way that balances out the breach. As clarified by Arts. 402 and 403 of the BrCC, the compensation for economic losses is broad, including any positive damages (*damnum emergens*), as well as any missed economic profits (*lucrum cessans*), directly linked to the breach.⁴³⁴

Contractual torts (Arts. 389 to 393 BrCC) require two basic elements: 1) default of a contractual obligation for which the debtor was responsible; and 2) a causal link between the frustrated obligation and the damage caused to the creditor. There is no need for

⁴³⁰ da Silva Pereira 2013: 45.

⁴³¹ Tartuce 2014: 332.

⁴³² Machado & Santa Inês 2012: 3

⁴³³ Wald & Giancoli 2012: 108.

⁴³⁴ Venosa 2013: 346-347

“culpa” or any other subjective evaluation of the debtor’s intent.⁴³⁵ Should the dispute be brought before court, the burden of proof is borne by the plaintiff for the facts that constitute his rights and by the defender for elements and facts that preclude, modify or extinguish the right of the plaintiff (Art. 333 I and II Brazilian Code of Civil Procedure). To summarize, should the creditor start a claim against the debtor to obtain compensation for a contractual breach, it is up to him to prove the existence of his right, together with the frustration of the obligation and the damage therein. It is then the duty of the debtor to present evidence of the contrary. A debtor shall not be held liable for *cas fortuit* and *force majeure*, except if the terms of the contract expressly state his responsibility for the event (Art. 393 BrCC).

Under the general theory of obligations, however, the determination of whether an obligation is fulfilled may entail an assessment of the nature and object of the obligation, as well as the means or methods of its performance. Traditionally, Brazilian private law has divided obligations in three separate but often overlapping categories: *dar* (Arts. 233-242 and Arts. 243-246 BrCC), *fazer* (Arts. 247-249 BrCC) and *não fazer* (Arts. 250 and 251 BrCC). Nevertheless, for the purpose of torts there is a preference to make a distinction between obligations of means and of result,⁴³⁶ as these categories simplify verification of the fulfilment of an obligation. An obligation of result is only fulfilled when the agreed upon result is achieved. As a result, if the plaintiff can prove that the result of the obligation was not attained, he will be compensated for the contractual tort, taking into account the circumstances of the case. In this case there is no need to consider or prove *culpa* of the debtor: the unperformed obligation generates liability. Obligations of means, on the other hand, are only evaluated on the basis of diligence and good faith. Since there is no presumption of culpa, it is up to the creditor to prove that the obligation was not adequately fulfilled, proving the debtor’s performance was in contradiction with or below the standards of the *bonus pater familias*⁴³⁷ and the fair expectations of the contract.

For the purpose of this report, i.e. the application of the concept of due diligence and care in security incidents involving business, ISPs and software vendors, we shall narrow our analysis to the cases under consideration. A contract of purchase and sale which requires a security solution to be deployed by a given corporation, for instance, always includes an expectation of diligence and care linked to contractual good faith. A company is expected to carefully evaluate the offers in the market and choose the adequate solution for ensuring security of its business. The more sensitive the activity carried out by the company and the more damaging adverse side-effects or spillovers of a security breach, the higher the thresh-

⁴³⁵ Wald & Giancoli 2012: 284.

⁴³⁶ Venosa 2013: 57.

⁴³⁷ Venosa 2013: 58.

hold of diligence. Moreover, a software company which commercializes security solutions must disclose all information that can influence the conclusion of the contract and set realistic expectations about what it can offer. It must act with transparency and objective good faith. If the agreement of purchase and sale is finalized and, shortly after, the company becomes victim of a cybersecurity incident causing data loss and material damage that should or could have been prevented if the purchased security solution had functioned properly, it can hold the software vendor liable for the loss. On the other hand, should the company consciously purchase security solutions which were recognized as outdated and obsolete in light of the state of the art, perhaps for the attractive price, the court can declare the lack of due diligence and care deployed in the given contractual relation. In both cases, the terms of the contract and the fair expectations therein are fundamental elements for the application of the law on contractual torts. The potential adverse effects of these security incidents on the lives of users and customers is analyzed in section 5.4.2.1.

Yet, the reality of cybersecurity makes the situation above quite complex. Although in Brazil rules of implied warranties prevail,⁴³⁸ express clauses of the contract may reduce or exclude liability of the software vendor for eventual security incidents. As explained by Stuber & Belluomini,⁴³⁹ Brazilian civil law allows for contracts to be ruled by the will of individuals, and if parties decide to exclude or limit responsibility, this must be explicit and in detail. Yet, and even if such detailed and explicit clauses are part of the contract, they may still be denied efficacy if one of the parties is in a financial, economic or cultural superior position.⁴⁴⁰ Moreover, proving the causal link between the faulty product and the damage as well as measuring the damage itself require specialized computer forensics. Finally, regardless of the faulty performance of the contract, third parties are, or may be, involved in the incident, e.g. the cybercriminal behind the attack, reckless employee inside the corporation. Clearly, the above circumstances can only be evaluated in the concrete case. Nevertheless, there is room in Brazilian civil law to hold business, software vendors, and ISPs liable for insufficient diligence and care in relation to security incidents. Lack of case law on the matter, however, lends uncertainty as to how these elements and circumstances will be treated in court.

5.4.1.2. *Extra-contractual torts*

The Brazilian Civil Code covers both contractual and extra-contractual torts. The first set of provisions is largely presented under Title IV, Book I, Special Part; provisions on extra-contractual torts are to be found under Title IX, Book I, Special Part. Yet, the Civil Code is to be

⁴³⁸ Stuber & Belluomini 2002: 133

⁴³⁹ Stuber & Belluomini 2002: 143.

⁴⁴⁰ Stuber & Belluomini 2002: 143.

read as a holistic instrument. While the general principles of tort law are applicable to both categories, contractual torts have more detailed provisions to measure the performance, as well as predetermined standards for other duties and for the burden of proof. Under Brazilian law, extra-contractual torts can derive either from subjective or objective responsibility. The general rule on torts, which introduces subjective responsibility as a default standard, is presented in Art. 927 BrCC: whoever commits an illicit act in the terms of Arts. 186 and 187 is liable for the damages thereof. The unique paragraph to Art. 927 introduces objective responsibility for the cases specified by law in which the activity of the agent generates, by its own nature, risks to others. Subjective responsibility (Arts. 186 and 927 BrCC) requires the presence of a subjective element referred to as *culpa* (fault), which includes *culpa stricto sensu* and *dolo* (*dolus*).⁴⁴¹ Moreover, a limited number of defences may excuse the tort, namely state of necessity (Art. 188, I, BrCC), *cas fortuit*, *force majeure*, and exclusive fault of the victim (Art. 945 BrCC) or of a third party (Art. 930 BrCC), whereby some defences are admissible only in specific types of cases. The same obstacles to ascertaining the liability of business, software and hardware suppliers and ISPs for their security choices under a contractual tort are present here: it is difficult to prove the causal link between the damage and the security vulnerability, liability defences will have to be assessed, and there is a lack of case law to shed light on these issues.

Under Brazilian law, *culpa stricto sensu* (Aquilian liability) regards intent to perform the action that led to the damage; the damage itself was not intended by the agent but was foreseeable in the circumstances of the case. *Culpa stricto sensu* consists of three essential elements: a) an error in an intended action, b) the foreseeability of the result and c) a lack of care, caution, or diligence. The foreseeability of the result is required for *culpa*; without it, there is no unlawful conduct. In extra-contractual torts, the victim has to prove that the wrongdoer acted with *culpa stricto sensu*.⁴⁴² The intention of the agent, however, does not play a role in the calculation of the compensation, in contrast to criminal law, under which *dolo* is always punished more severely.⁴⁴³ Here the legislator aimed to re-establishing the situation as it was before the tort was committed, thus protecting the victim.⁴⁴⁴ As a result, the compensation for tort damages as prescribed in Art. 944 is broad, following the principle of full compensation enshrined under Art. 402.⁴⁴⁵ This is to say that compensation

⁴⁴¹ Wald & Giancoli 2012: 285.

⁴⁴² Wald & Giancoli 2012: 201.

⁴⁴³ Notwithstanding, Brazilian doctrine recognizes different types of *dolo*, namely direct *dolo* (if the action is aimed at achieving the illicit result), necessary *dolo* (if the agent aims at a licit result, but is aware that his action will inevitably lead to an illicit result), eventual *dolo* (if an agent aims at a licit result, but understands that an eventual illicit result may follow from his action).

⁴⁴⁴ Salim 2005: 99.

⁴⁴⁵ Wald & Giancoli 2012: 242.

for extra-contractual torts also include *damnum emergens* and *lucrum cessans*, meaning all damages that were actually caused to the victim, as well as the loss of reasonably expected economic gains.

An agent acts with *dolo* if he is conscious of the unlawful nature of the action and the damage it might cause. In this case, the conduct of the agent is itself unlawful, whereas in *culpa stricto sensu* the action is diverted towards an unlawful end because of the lack of care, caution and diligence deployed by the agent. Consciousness of the wrongful act and the eventual damage are not to be confused with a willingness to provoke the result. *Dolo* merely requires that the damage is predictable and accepted by the wrongdoer at the moment of the action, regardless of whether he wished for the damage to take place. At present, the distinction between *culpa stricto sensu* and *dolo* is merely theoretical and negligible in practice. As highlighted above, the intention to commit the wrongful act and consciousness of the wrongful act are not taken into account when ascertaining the compensation for the tort. Thus, it makes more sense to refer to *culpa* as comprising the two modalities described in this section.

For the purpose of general tort law, including both contractual and non-contractual torts, a distinction between different levels and types of *culpa* is made in doctrine and case law. For the scope of this paper, it is relevant to discuss three circumstances under which the agent's fault is presumed. These are *culpa in eligendo* (Art. 932 BrCC), *culpa in vigilando*, and *culpa in custodiendo*. *Culpa in eligendo* stands for the lack of care, attention, caution or diligence attributable to an agent who chooses badly and trusts a third person with the performance of an obligation. *Culpa in vigilando* entails the fault of an agent for lack of care, attention, diligence or caution towards the actions of another party for whom he is legally responsible. *Culpa in custodiendo* takes place when the agent breaches a duty of care under which he was responsible to oversee and ensure proper control and security/safety of a thing, animal or person.⁴⁴⁶ Modern Brazilian scholarship affirms that the theory of *culpa* has lost its place in civil law, as the Brazilian Civil Code of 2002 converted most of these conducts into objective responsibility. Additionally, the very idea of a *bonus pater familias* or reasonable person reflects the legal fiction of a standard that is much closer to the values and actions of the judge himself/herself, than to those of a regular citizen who makes honest mistakes.⁴⁴⁷ Altogether, the decadence of the model of *bonus pater familias*, the insufficiency of the traditional tort system and the obsolete concept of *culpa* are pushing tort law towards a new paradigm.

As noted by Anderson Schreiber,⁴⁴⁸ there is a tendency to objectify torts. The traditi-

⁴⁴⁶ Schreiber 2009: 39

⁴⁴⁷ Schreiber 2009: 39

⁴⁴⁸ Schreiber 2009: 31.

onal theory of torts based on the three pillars of unlawful act, causal link and damage is incapable of repairing the diversity of damages caused by the risks of modern society. The risk society presents a new context in which third parties suffer damages and losses without there necessarily being an unlawful act. From this perspective, the criterion of proper care and diligence, which help to establish whether an act is unlawful, is set aside. In modern tort law and in tort law as contained in the BrCC, the creation of risks as an intrinsic collateral effect of any business activity brings about an objective responsibility of the agent for the damages thereof (Art. 927, §1, BrCC). The challenge, however, is to define and concretise this norm. Art. 927 par. 1 of the BrCC is often understood as an open objective responsibility clause. The theory of risk only applies to damages caused by an activity which is normally performed by the agent. Therefore, the meaning of activity and *normally performed* are the crucial elements⁴⁴⁹ of this open clause. They should be interpreted in a manner which restricts the risk of liability to a reasonable level. The term ‘activity’ is understood as a regular, reiterated, professional or business oriented activity for economic purposes.⁴⁵⁰ ‘Normally performed’ refers to any non-isolated, irregular, transitory activity that forms a close link to its object.⁴⁵¹ The modern legal framework of Brazilian tort law, thus, is one which embraces both damage and fault as coexisting sources of liability.⁴⁵²

Even if the law imposes liability for risks that are normally created by the regular business activities, in certain cases damages will arise without being a result of unlawful acts or risks of the regular activity of the agent. In these cases, the victim is left in a limbo: he or she has suffered damage but there is no agent liable for the act. Refusing compensation for these damages would amount to leaving the victim to its own “bad luck”. In this context, scholar Giselda Hironaka has introduced the concept of presupposed fault (*culpa pressuposta*), which focuses on repairing, compensating, deterring and preventing damages. The scholar advocates that tort law should no longer refuse to compensate unfair damages caused by lawful actions.⁴⁵³ This is particularly prominent problem in damages caused in relation to IT security incidents, as noted by Wald and Giancoli.⁴⁵⁴ The difficulty in attributing the damage to an individualized agent, for instance, in damages caused by malware infection, has led to an undesirable social scenario.⁴⁵⁵ For the authors, the current stage of theory of risk, causality and damages in Brazilian law is insufficient to fully regulate

449 Beraldo 2004: 317-340: 320.

450 Wald & Giancoli 2012: 226.

451 Beraldo 2004: 317-340: 321.

452 Hironaka 2007: 35.

453 Hironaka 2007: 35.

454 Wald & Giancoli 2012 : 294.

455 Wald & Giancoli 2012 : 294.

torts caused in information systems,⁴⁵⁶ which are extremely difficult to measure. However, the theory of *culpa pressuposta*, which sets aside the requirement of unlawful act and could collaborate to a better understanding of the social costs of cybercrime, has not been unanimously welcomed by doctrine or legal practice and cannot find support in statutory law. Yet, as noted above, scholars are rightfully calling for further development of tort law and their application to the special characteristics and damages caused in cyberspace.⁴⁵⁷ As case law and doctrine develop and more cases are brought to courts, it is likely that the matter will be given further appreciation in the country.

5.4.1.3. Preliminary conclusions regarding key actors

For the key actors discussed in this report (businesses, ISPs and software vendors), and given the gradual move in Brazilian law towards a liability regime focusing less on fault and more on compensation, duties of care and diligence may appear to become less relevant. The choice for an objective system of liability removes the importance of the intention of the agent, therefore reducing the role of care and diligence as a means to minimize and/or exclude the responsibility of the wrongdoer on a subjective level. But subjective responsibility continues to coexist with situations that call for objective responsibility, and the doctrine remains largely applicable in contractual law and the law on obligations of means. Industry practice has long contracted insurance companies to guarantee business against liability from any damages. However, Brazilian law does not require companies to contract insurance,⁴⁵⁸ although business practice and public procurement often calls for such coverage before contracts are signed. Regardless, Brazilian law appears to accept a higher level of liability for the key actors involved, when compared to other countries. Liability would be assumed sooner, whether under an actual subjective responsibility akin to a duty of care and diligence, or under objective responsibility (which arguably might be an abstraction from such duties). Moreover, Brazilian law protected the victim against disputes between the agent and third parties. Art. 930 of BrCC establishes that if an agent causes damage that can be attributed as fault of a third party, the agent shall have the right to reclaim the damages paid to the victim. This is to say that when the elements of torts are present, third party liability disputes shall not hinder the right of the victim to be compensated for the damage. In the end, only case law can provide sufficient guidance on the extent to which, and circumstances in which, the lack of diligence and care for IT security can be classified as a lawful act or otherwise impose liability.

⁴⁵⁶ Wald & Giancoli 2012 : 295

⁴⁵⁷ Wald & Giancoli 2012 : 295.

⁴⁵⁸ Stuber & Belluomini 2002: 147.

5.4.2. Consumer Law

5.4.2.1. General description of consumer law

While many jurists have interpreted consumer and civil law as mutually exclusive sets of legislation, the current understanding set forth by the new BrCC and current scholarship is one of a *dialogue des sources*.⁴⁵⁹ Therefore, should the same legal issue be concurrently regulated by both codes, civil and consumer codes must interact to find the best legal solution for the case.

In principle, however, the BrCDC is a special set of laws that only applies to *consumer relations*. This is any relation in which it is possible to identify a negotiation on the delivery of a product or service between a consumer and a supplier for direct or indirect remuneration. The consumer relation, therefore, requires the presence of at least three elements (consumer, supplier, and product/service), which are all defined in Arts. 2 and 3 of the BrCDC. In an attempt to surmount the inevitable challenges of capturing real life relations in legal terms, the BrCDC gave broad definitions to these elements with the purpose of embracing the dynamics of the commercial relations of modern society. Special legislation has been enacted to regulate and integrate specific consumer relations subject to the BrCDC, including the Presidential Decree 7.692/2013, which regulates e-commerce as a consumer relation under the framework of the BrCDC.

It is important to note that the concept of supplier as defined by Art. 3 of the BCDC is a generic term which, for the purpose of the law, comprises manufacturers, producers, and retailers, among others, both as natural and as legal persons. The fact that many ISPs offer “free” services does not exclude application of the BrCDC. The gratuity of the service provided by some ISPs is often “illusory”, since in the vast majority of cases there is an indirect remuneration offered by a third party⁴⁶⁰ (e.g. via ad and marketing services). In addition, the commercial value of a website is directly linked to its popularity. As a result, users create value for the website owners,⁴⁶¹ who can, for example, ask higher prices for displaying ads. Despite the image created by Internet actors that their service is for free, it is contrary to common sense and business logic that a company, whose main activity is to generate profit, can offer products or services in a purely altruistic manner.⁴⁶² The provision of an online service or product will often entail the exchange of data, hardware space,⁴⁶³ or audio and image files, among other digital goods. Back to the concepts introduced by the

459 Tartuce & Neves 2014: 41.

460 Martins 2014: 1.3 O conceito de fornecedor e os provedores gratuitos.

461 Martins 2014: 1.3 O conceito de fornecedor e os provedores gratuitos.

462 Martins 2014: 1.3 O conceito de fornecedor e os provedores gratuitos.

463 Martins 2014: 1.3 O conceito de fornecedor e os provedores gratuitos.

BrCDC, Art. 2 also gives the term consumer a far-reaching interpretation. Under Brazilian law, “consumer” is any natural or legal person acting as the final recipient of a product or service in a consumer relation. In fact, the BrCDC introduced the very concept of bystander to Brazilian law,⁴⁶⁴ extending its beneficial treatment to all third parties affected by a consumer relation. In addition, the duty to compensate third parties affected by the contractual relation – bystanders – is also present in Art. 931 of the BrCC, which should be read in conjunction with the BrCDC to offer the most beneficial treatment to the consumer.⁴⁶⁵

The BrCDC was drafted with the clear purpose of safeguarding consumers in any given consumer relation, as described by the law. Needless to say, the main principle of the BrCDC is the principle of consumer protection (Art. 1 BrCDC), under which every norm of the BrCDC seeks to protect and defend the consumer.⁴⁶⁶ For Tartuce & Neves, this principle has three direct consequences:⁴⁶⁷ 1) mandatory application of the BrCDC to consumer relations; 2) room for intervention of the Public Prosecutor (Parket) in any issue involving a consumer relation as a consequence of Art. 82, II, Brazilian Civil Procedure Code; 3) automatic application of consumer law by the courts.⁴⁶⁸ The principle of the vulnerability of the consumer (Art. 4 par. 1 BrCDC) recognizes the unbalance between the consumer and the supplier of a product or service. The presumption of consumer vulnerability is thus *iure et de iure* and cannot be waived or set aside in any circumstance.⁴⁶⁹ By acknowledging the intrinsic vulnerability of the consumer, the BrCDC fulfils the constitutional principle of isonomy.⁴⁷⁰ The inevitable vulnerability of the consumer is both technical and economic: the supplier is always in a better position to understand and decide on the product or service which is commercialized, and is frequently in a better economic position than the consumer.⁴⁷¹ One noteworthy aspect of the broad sense given to the term ‘consumer’ in the BrCDC is that it does not exclude business from classifying as a ‘consumer’ in the terms of the law, as is clear from the text of Art. 2 of the BrCDC.⁴⁷² Other important principles put forward by the BrCDC include dignity, transparency, good faith, safety, security, information and solidary liability (i.e. joint and several liability) of suppliers. The latter is particularly important to this analysis.

464 Tartuce & Neves 2014: 76.

465 Tartuce & Neves 2014: 147.

466 Rizzato 2012: 677.

467 Tartuce & Neves 2014: 42.

468 In this regard, Tartuce & Neves defend the vinculative decision n. 381 of the Supreme Court to be void, for being in clear contradiction with the principles of the Consumer Protection Code.

469 Tartuce & Neves 2014: 43.

470 Rizzato 2012: 178.

471 Rizzato 2012: 179.

472 Art. 2° Consumer shall be any natural or juridical person that obtains or makes use of a product or service as the final recipient.

The BrCDC embraces the principle of adequacy of a service or product, which is embedded in multiple provisions of the code (Arts. 4, II, d, Art. 8, Art. 18, Art. 19, Art. 20 and Art. 24). The guarantee of adequacy offers security regarding the functioning, performance, quality, and durability of the product or service,⁴⁷³ as well as the nonexistence of a risk to the consumers' physical, psychic and financial well-being.⁴⁷⁴ The adequacy principle thus objectifies the duty of care and diligence in the conception, execution, production, manufacturing, and commercialization of the product or service. In relation to ISPs, companies bear an overall duty to deploy technologies that match at least the minimum adequate security requirements in light of the state of the art.⁴⁷⁵ It is only logical that every supplier offering a product or a service to the market, via remuneration or indirect benefit, deploys the same minimum adequate safety and security standards (e.g. any business or software company). A failing to do so results in direct liability for the damage which is directly or indirectly caused to the user, or at least in contributory liability for the act of a third party that was not prevented⁴⁷⁶ due to the security vulnerability. Under the system of the consumer protection framework, the security requirement comprises the need for maintenance and updates of the infrastructure and software so as to minimize any damage that may be linked to insufficient security mechanisms, as well as damage related to their exploitation by a third party.

In relation to torts, the BrCDC integrates important theories on liability, including the theory of full compensation, the enterprise risk theory, and theories concerning risk of the activity and the development. The BrCDC therefore recognises that the economic activity and the means of production and performance of a service inexorably create risks to consumers, regardless of the intention or performance of the supplier. Consequently, the BrCDC adopts objective responsibility as the default system of consumer torts (Arts. 12, 14 and 18, *caput*, BrCDC). As a result, consumer torts require the presence of three elements: a defective (*defeito*) or vicious (*vício*) service or product; damage; and a causal link between the damage and the defective/vicious service or product. The elements of causality and damage are the same as those used in other areas of torts, but the concept of defective and vicious product or service in the BrCDC deserves further consideration, as it entails different levels of compensation for potential damages. A *vício* in a product or service is an issue on quality or quantity that renders the product or service inappropriate, less valuable, or inadequate for the purpose for which it was intended,⁴⁷⁷ whereby the purpose is deter-

473 Rizzato 2012: 426.

474 Efig 2000: 103. Leonardi 2005: 65.

475 Leonardi 2005: 51.

476 Leonardi 2005: 51

477 Rizzato 2012: 229.

mined by the information which the consumer received and by his fair expectations (Art. 18 BrCDC). A defect (*defeito*) is an aggravated category of product or service liability (Art. 12 and 14 BrCDC). A defective product or service is one that combines the damage of a *vício* with material, moral, reputational or esthetical damage.⁴⁷⁸ Consequently, the compensation for a product or service defect is higher. Damages caused by defective products or services are known as *fato do serviço/produto*, or simply consumer accidents.

Finally, it is important to notice that Art. 51, inc. I, BrCDC declares void any contractual clause that hinders, exonerates or narrows the responsibility of the supplier for the vices of the product or service, as well as any clause that may waive or alienate consumer rights. In short, Art. 51, inc. I, BrCDC vetoes any non-liability or non-compensation clauses by declaring them void *iure et de iure*. Liability can only be waived in cases of exclusive fault of the victim or contributory negligence.⁴⁷⁹ Art. 10, §1, II of Law 9.609/1988⁴⁸⁰ (Brazilian Software Act) expressly introduces the same veto in the context of software licenses. Therefore, any contractual clause intended to exempt the contractual parties of a software license contract from eventual third party actions related to *vício*, *defeito* or violation of copyrights is void.

5.4.2.2. Preliminary conclusions on consumer torts

The ‘consumer torts’ in Brazilian law effectively assume an extensive regime similar to product liability, but with the understanding that it applies primarily to contract parties (and not to third parties), may also apply to ‘weaker’ businesses, and applies to products and services alike. Coupled with the fact that this form of liability can not be limited contractually, this provides a powerful form of liability. It may lead to further liability for software vendors, ISPs and business where they have been neglecting a duty of care and diligence. In more detail, the following can be argued.

The line between *vício* and *defeito* relies on the produced damage itself, rather than on nature of the issue. For instance, a given anti-virus software vulnerability can be exploited to make the software itself inoperable, e.g. incapable of detecting new malware. However, the same vulnerability could also be used to install a key logger, therefore collecting sensitive credentials to enable bank fraud. In both hypothetical cases, the issue present in the product supplied by the software company is the same, but the effects are substantially different. In the first case, the damage caused to the consumer is limited to the actual functionalities of the product: the software has a *vício*. The vulnerability, exploited by a third party, provoked limited damage to the consumer. In the second case, the damage surpasses-

⁴⁷⁸ Rizzato 2012: 230.

⁴⁷⁹ Tartuce & Neves 2014: 228

⁴⁸⁰ Original version in Brazilian Portuguese: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm

ses the sphere of product usage: the software has a *defeito*. The vulnerability, exploited by a third party, has spillovers on the material assets and on the private life of the user.

In the case of a vicious product, both the manufacturer and the retailer will share liability for the event.⁴⁸¹ Here, the consumer can request the replacement of the flawed pieces of the product. If this substitution does not occur within the prescribed period of 30 days, the consumer can request, at his own discretion (Art. 19. 1): I – the substitution of the product for another of the same category, in perfect condition; II – the immediate reimbursement of the expenses, with corrections, without prejudice to an eventual damages claim; III – a proportional reduction in price. In the case of a vicious service, all actors involved in the provision of the service are jointly liable for the event.⁴⁸² Art. 20 determines that whenever a service presents quality issues that render it unusable, less valuable, or different from what was indicated in the offer or advertisement, the consumer can request, alternatively and at his own discretion: I – the re-execution of the service, when feasible and without additional costs; II – the immediate reimbursement for the amount paid, with corrections, without prejudice of eventual damages claim; III – proportional reduction in price.

Under the BrCDC, the defectiveness of a product imposes direct and immediate liability on the manufacturer for the damages caused by the product, whereas the liability of the retailer is only mediate and subsidiary.⁴⁸³ In the case of a defective service, all actors involved in the provision of the service are jointly liable for the damages caused to the consumer.⁴⁸⁴ The damage caused by a defect is constructed in accordance with the principle of full compensation, including any material, moral, esthetical and reputational damages.

5.4.3. *Administrative Law*

5.4.3.1. *Marco Civil*

After five years of discussion, the first law dedicated to regulating the Internet in Brazil, the so-called Marco Civil (Law 12.096/2014),⁴⁸⁵ was finally approved in April 2014. The Marco Civil is a framework legislation that laid the foundations of Internet governance in the country, setting forth important regulatory principles such as net neutrality, privacy, data protection, security, freedom of expression, and liability for activities online (Art. 3, I to VI). Despite the improvements brought by the legislation, there is still need for further

⁴⁸¹ Tartuce & Neves 2014: 121.

⁴⁸² Tartuce & Neves 2014: 121.

⁴⁸³ Tartuce & Neves 2014: 121.

⁴⁸⁴ Tartuce & Neves 2014: 121.

⁴⁸⁵ An English translation is available at <https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf>

regulation via presidential decree.⁴⁸⁶ At this point, it is not clear how courts are supposed to interpret and apply the new law. For the purpose of this paper, we shall restrict our attention to the liability framework introduced by the Marco Civil.

Although the Marco Civil establishes the liability of agents for their activities online as a fundamental legal principle for the use of the Internet in Brazil (Art. 3, VI), its liability provisions are rather short and insufficient to cover the variety of actors and the risks which are created by their activities online.⁴⁸⁷ In this regard, the Brazilian legislator missed the opportunity to regulate important security aspects of the Internet, in contradiction with the principle of security, stability and functionality of networks (Art. 3, V). Falling short in examining the important role played by ISPs and other Internet actors in cyber security, the Marco Civil limits the discussion of ISP liability to content generated by third parties (Arts. 18 to 21). Based on Art. 18, Internet Access Providers are not liable for torts constituted by content generated by third parties. Moreover, Art. 19 establishes that an ISP is only liable for damages caused by content generated by a third party if it fails to take the necessary, reasonable measures to make the disputed content unavailable after a specific court order. The only exception is the case of images, videos or other materials containing nudity or sexual acts of a private nature, in which case the ISP will have to take down the concerned material following a request from an interested person without requiring a court order (Art. 21). The law does not address liability issues other than those related to honour, reputation, privacy and other personality rights (Art. 19, par. 4 and Art. 21). The Marco Civil demonstrates the current difficulty of striking a balance between the principles of net neutrality (Art. 9), privacy and confidentiality of communications (Art. 10), freedom of expression, and security. In a successful attempt to safeguard the first two principles, the legislator missed the chance to define the security standards and responsibilities applicable to Internet actors. There is a need for authoritative interpretation on how the liability system introduced by Arts. 18 to 21 of Marco Civil interacts with the framework of the BrCDC.

There is today an absolute gap between decisions addressing the security of networks and the consumers torts that define to what extent it is part of the risk of the activity performed by ISPs to prevent security incidents. There is also a clear need to differentiate between the different types of ISPs and the role each one of them can play to ensure and promote a secure Internet. The current understanding of the legislator, as evidenced by the Marco Civil, is to see ISPs as intermediaries who are seldom liable for any damages. Because the activity of each type of ISP may differ, the legal expectations of security shall be

⁴⁸⁶ On 28 January 2015 the Brazilian Ministry of Justice launched two online public consultations, one regarding a Draft Data Protection Bill and the other concerning the Marco Civil draft presidential decree. See <http://participacao.mj.gov.br/dadospessoais/> and <http://participacao.mj.gov.br/marcocivil/>. Access 17 February 2015.

⁴⁸⁷ Cf. also the analysis in Gallardo & Gálvez 2011.

analyzed in light of their means and capabilities, and not solely on the basis of the scope of business of the agent. This should be extended to any business or software vendor that can contribute to IT security. As an intrinsic element of any service or product, security and safety generate fair and reasonable contractual expectations which are threatened by the lack of allocated liability in the private sector. On the one hand, realistic expectations must take into account the fast paced development of cyber-threats and the fact that some incidents are still unpredictable or unavoidable by the service or product supplier, but on the other hand, there is today a void in tort law as damages continue to take place with no sharing of the risks between victims and the involved private sector.

For instance, considering the issue of ransomware, it does not seem reasonable to hold ISPs liable for the incident. A duty to contain the distribution of malicious content would require ISPs to monitor Internet traffic and content production, which contradicts the principle of net neutrality and can create serious challenges for online freedom of expression. The difficulty in balancing such principles, however, must not be an excuse for inertia. In many cases, there are less invasive tools and solutions that can be used by ISPs to detect malicious traffic and content. Yet, one shall not forget the criminal responsibility of the author of the offence, who can also be held liable for civil torts and eventually share any liability for damages with the Internet actor that created the opportunity for the crime to take place. In a DDoS attack, for instance, an ISP has better access to means and methods of detection. The excessive flow targeting a certain website can be observed and monitored before it actually takes place. ISPs, more specifically backbone infrastructure and access providers, can use several tools to divert or prevent the damage without creating spillovers.

5.4.3.2. *National Telecommunications Agency Res. 632/2014*

The Brazilian National Telecommunications Agency (ANATEL) is the public administration entity responsible for the regulation of telecommunication services in the country. Created by the Telecommunications Act (Law 9.472/1997), ANATEL is an administratively independent and financially autonomous institution. The agency has widely regulated telecommunication services in the country. For the purpose of this study, it is worth mentioning the recent ANATEL Res. 632/2014, which introduced the general regulation of consumer rights in telecommunication services. As provided in Art. 3 (I, V, VI, VII and XI), consumers have the right to: I. access and fruition of services according to the contracted standards and quality; V – confidentiality and secrecy of communications; VI – non-suspension of service without prior solicitation, except as provided by the law; VII – privacy for billing purposes and use of their personal data; XI – compensation for damages. Moreover, telecommunication services are subject to objective responsibility for the damages caused to their users, based on Art. 37, §6ffl of the Brazilian Federal Constitution and Art. 14 of the BrCDC.

5.4.4. Criminal law

The main issue presented by Brazilian criminal law is the scarcity of specific cybercrime provisions. Despite recent amendments on online protection of children, only hacking and unauthorized system interference are covered by the Brazilian Criminal Code. These provisions, added via Law 12.737/2012, have not resulted in any final conviction, causing a gap in case law on crimes against information systems. There persists a misconception that the current version of the criminal code and other special laws are sufficient to address the crimes committed online. However, the question is not whether the current legislation is applicable, but rather whether it is sufficient and adequate to deal with cyber criminality – and it is not. In this regard, there seems to be enough room for improvement in Brazilian law: the lack of provisions which criminalize the primary offence also result in a lack of accountability for the actions of actors that indirectly contribute to the event.

A strict interpretation of criminal law combined with the limited application of the cybercrime provisions precludes a clear possibility for criminalization of the activities of ISPs, business and software vendors which display a lack of diligence and care. However, we analyse below whether and how a duty of care and diligence could be linked to cybercrime offences by exploring the concepts of commissive crime by omission (*crime comissivo por omissão*), aiding and abetting, and the duty to put in place security mechanisms.

The concept of commissive crime by omission in Brazilian law follows the German tradition of a guarantor who can help prevent illicit activities from taking place or from achieving the planned result. This is described as the doctrine of ‘norma de dever de segundo grau’⁴⁸⁸ (a second-degree duty, freely translated) and targets the agents which hold a special protective relation towards the protected right. The guarantor of the right is thus in the position to prevent the violation of the right. For an agent to commit a commissive crime by omission, three elements must be demonstrated in conjunction with the illicit activity, namely: 1) the power to act; 2) the preventability of the result; and 3) a duty to prevent the result. It is possible to argue that there are cases in which ISPs, software vendors, and business have a *de facto* power to act. For instance, a software vendor can fix the vulnerability of his product or service upon becoming aware of the issue, businesses can restrict the access of employees to certain devices and deploy improved software and hardware security, and ISPs can install honeypots, filter and divert malicious traffic, block access to suspicious websites, and disconnect malicious users. The second element, preventability of the result, is particularly difficult in a cybersecurity environment, as discussed before. This will require specialized knowledge of computer forensics and malware intelligence to verify whether the considered actions could have prevented the harmful event. Finally,

⁴⁸⁸ Bitencourt 2012: 265.

there has to be a legal duty to prevent the result. The legal duty to provide network security, however, appears not to exist in current legislation.

Art. 13 par. 2 of the Brazilian Criminal Code defines the bearer of a the duty to act as anyone who a) has a legal obligation of care, protection or vigilance; b) assumed the responsibility to prevent the result; or c) with a previous behaviour, created the risk to that led to the result. The challenge is to find a legal provision that establishes a duty to act in cases of security threats for ISPs, software vendors, or businesses. It is not clear what legal sources other than the Criminal Code could be used to infer the existence of this duty and whether the Marco Civil, by establishing the principle of network security, introduces such a duty for Internet actors. This appears to go against the intention of the legislator, not to mention issues with principles of criminal law such *nulla poena sine lege* and the prohibition of *analogia in malam partem*.

Finally, the concept of aiding and abetting does apply to the cybercrime offences in Brazilian law. By default, criminal offences require *dolo* of the agent; only if specifically described by law will an act be criminalized in the presence of *culpa* instead of *dolo*. This is not the case for the crimes of hacking and unauthorized interference with a system, which require *dolo* of the agent. Aiding and abetting would therefore require the same harmful and conscious decision from the second agent. This is to say that if businesses, software vendors or ISPs were to be considered offenders under current legislation, these actors would need to display *dolo* in creating the opportunity for the cybercrime, meaning that they would need to intentionally create or enable vulnerabilities with the purpose of supporting the action of the cybercriminal. In this case, it is inevitable that such actors will also be held criminally liable for the damages caused to society. However, the mere lack of care and diligence in ensuring the security of networks cannot amount to cybercrime *dolo*. The considered agents therefore cannot be considered co-authors of the crime, nor aiders and abettors.

5.4.5. Conclusion

Brazilian law appears to be favourable to assuming legal duties of care and diligence. Furthermore, the 'product liability' rules in the BrCdC encompass products as well as services, apply to private individuals as well as business users, and allow compensation for certain non-material damages. This provides a solid basis to assume that there is enough room under current private law to hold businesses, software vendors and ISPs liable for damages caused to users by security vulnerabilities, even if the damages are linked to the activities of third parties that exploit those defects in security. The extent to which actors are in fact liable, however, remains to be seen, as there is no case law on this particular matter. This may also be due to uncertainty to what kinds of non-material damages are compensated: does this also include loss incurred by defective software? Furthermore software

vendors may by the wording of the licence provisions influence the expectations regarding the software, resulting in a low standard of ‘adequacy’ of the software. With regard to criminal law, there seems to be no room to hold ISPs, software vendors or businesses liable for actions which were not committed with direct criminal intent (*dolo*), such as a mere lack of proper diligence and care for IT security.

5.5. Czech Republic

The Czech Republic has a continental, civil law system belonging to the Germanic branch of civil law. The main characteristics of the Czech legal system are that (1) the principal fields of law are codified; (2) the sources of law form a hierarchical structure; and (3) only written laws (statutes adopted by the Parliament and (‘sub-statutory’) regulations adopted by the executive) are recognized as formal sources of law.^{489 490} Similar to other former Eastern bloc countries, the Czech legal order has been influenced by the period of Communist rule and has been undergoing a dynamic transition over the last twenty-five years to accommodate the democratic institutions, market economy and private property. The recent enactments of the Criminal Code (TZ) in 2009, the Civil Code (NOZ) in 2012 and of special laws such as the Cybersecurity Statute (2014) are interesting to study in relation to cybercrime since they were presumably tailored to fit the needs of a modern society, including the fight against cybercrime. It was inspired by legislative trends in other countries. A drawback is the lack of case law for the new legislation, which at present is still largely untested in legal practice.

5.5.1. Civil law

The civil law of the Czech Republic has historically been influenced mainly by the Austrian Civil Code (ABGB).⁴⁹¹ Until 1918, the Czech lands were part of the core of Habsburg Austria. Austrian Civil Law remained in force after the creation of the Czechoslovak Republic in 1918 due to the difficulty of unifying the Austrian written civil law used in the Czech lands and the Hungarian customary law that was used in Slovak areas. This state of affairs ended in 1950 when the communist regime adopted a temporary civil code to suit the needs of the newly established socialist regime. In 1964, the temporary civil code was replaced by a civil code (OZ)⁴⁹² based on socialist perspectives of civil law.⁴⁹³ The 1964 OZ remained in force

489 Although the decisions of the Constitutional Court and the Supreme Court have a significant influence over the legal system.

490 Pouperova 2013: at: http://www.nyulawglobal.org/Globalex/Czech_Republic1.htm. [accessed: 1 December 2014].

491 Allgemeines bürgerliches Gesetzbuch.

492 Hereafter 1964 OZ.

493 Lazar 2010.

in the Czech Republic until 31 December 2013 and is still in force in the Slovak Republic. Although it was heavily modified and amended after the political change in 1989 to accommodate the needs of market economy, private ownership, business freedom etc., its wording remained for the most part rooted in the circumstances of a socialist society.⁴⁹⁴

The need for a new codification was strongly felt by the early 2000s. After eleven years of work of the recodification committee of the Ministry of Justice,⁴⁹⁵ the new civil code (NOZ) (law no. 89/2012 coll.) was adopted by Parliament. It entered into force on the 1st January 2014. It was inspired by other European civil codes, in particular the Austrian ABGB and the German BGB. The NOZ specifies, modifies and extends the inadequate provisions of the 1964 OZ and codifies nearly the whole area of (substantive) civil law which was previously fragmented in several statutes.⁴⁹⁶

One of the significant changes of the NOZ is a stronger emphasis on contractual freedom. The 1964 OZ was rather unique among other European codes in the way in which it limited the freedom of contract parties.⁴⁹⁷ It contained a provision which prevented contract parties from waiving their future rights. As per § 574(2) of the 1964 OZ,⁴⁹⁸ any contract clause that prevented one of the parties to claim future damages or limited future liability was considered void.⁴⁹⁹ Parties could only waive the rights and claims they disposed of at the time of the waiver.⁵⁰⁰ The NOZ abandoned this far reaching limitation of contractual freedom, although the following limitations were retained in § 2898 NOZ:⁵⁰¹

- Liability for future breach of a person's natural rights⁵⁰² cannot be limited,
- Liability for future damage caused intentionally or by gross negligence cannot be waived,
- Clauses that preclude or limit future claims of damages by the weaker party are

494 Pouperova 2013: at: http://www.nyulawglobal.org/Globalex/Czech_Republic1.htm. [accessed: 1 December 2014].

495 Elias 2012: 21-32.

496 Elias 2012: 21-32.

497 Korbel 2012: at: <http://jinepravo.blogspot.nl/2012/03/frantisek-korbel-dnes-vysel-novy.html>. [ac-cessed: 1 December 2014].

498 § 574(2) of the 1964 OZ: "Dohoda, kterou se někdo vzdává práv, jež mohou v budoucnosti teprve vzniknout, je neplatná."

499 Svestka et al. 2013-VI: 883.

500 Handlar 2009: 659-663.

501 § 2898 NOZ: "Nepřihlíží se k ujednání, které předem vylučuje nebo omezuje povinnost k náhradě újmy způsobené člověku na jeho přirozených právech, anebo způsobené úmyslně nebo z hrubé nedbalosti; nepřihlíží se ani k ujednání, které předem vylučuje nebo omezuje právo slabší strany na náhradu jakékoli újmy. V těchto případech se práva na náhradu nelze ani platně vzdát."

502 The concept of natural rights is defined in §19 NOZ as rights that are innate to every person and can be recognized through reason a sense. These include rights such as the right to life, physical and mental integrity, dignity, health and healthy environment. (Svestka, Dvorak, Fiala, (VI) 2014: 884-886).

not allowed.⁵⁰³ It should be noted that the term ‘weaker party’ does not necessarily include only private individuals or consumers, but can also apply to a small or medium business when it is contracting with a large corporation.⁵⁰⁴ The weaker party is generally a natural or legal person who enters into a relation with a business entity which is not related to her own business activity.⁵⁰⁵

Apart from these three limitations, clauses which limit future liability are allowed if part of a bilateral agreement. Unilateral declarations do not directly lead to a limitation of liability, regardless of whether they are directed towards future damage. Such unilateral declarations can, however, be considered a warning of possible damage, which may result in an exclusion of liability of the party that issued the warning, particularly if the injured party acts against the warning despite being made aware of the risk. Hradek gives the example of a website administrator who issues a statement on his website that he is not responsible for its content. If a user copies the websites’ content on her computer and this causes damage, the liability of the website owner will in principle be excluded.⁵⁰⁶ The warning, therefore, effectively leads to an exclusion of liability, similar to an assumption of risk or contributory negligence in other legal systems.

5.5.1.1. *General and special preventive duties*

In the context of tort law, contract law, and particularly the existence of a duty of care and diligence, the NOZ contains two provisions that deserve particular attention. § 2900 establishes a general preventive duty and § 2901 establishes a special preventive duty.⁵⁰⁷

Non-compliance with these duties is seen as a breach of statutory duty and establishes statutory liability (see section 5.5.1.2. for the discussion of statutory/tort liability).

The general preventive duty imposes a general obligation on all subjects to act, if required by the circumstances of the case and the customs of private life, in such a way that the freedom, life, health and property of others will not be harmed without a justifiable reason. The duty applies both to contractual relations and to statutory duties. The general preven-

503 § 2898 NOZ.

504 Svestka et al. 2013-VI: 886.

505 Jansa, Otevrel 2014: 125.

506 Svestka et al. 2013-VI: 880.

507 § 2900 NOZ: “Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného

§ 2901 NOZ: “Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, má povinnost zakročit na ochranu jiného každý, kdo vytvořil nebezpečnou situaci nebo kdo nad ní má kontrolu, anebo odůvodňuje-li to povaha poměru mezi osobami. Stejnou povinnost má ten, kdo může podle svých možností a schopností snadno odvrátit újmu, o níž ví nebo musí vědět, že hrozící závažností zjevně převyšuje, co je třeba k zákroku vynaložit.”

tive duty can only be applied if there are no specific legal duties in place. It is generally not applied to, for example, traffic accidents, because traffic is regulated in great detail in other provisions.⁵⁰⁸ As a generally formulated obligation binding everyone's actions, it can potentially cover a wide range of human behaviour. Exactly what kind of standard of preventive care is expected has to be deduced from the decisions of the courts, in particular the Czech Supreme Court. Because the provision has only recently been enacted, it has not yet been applied by the courts. However, the 1964 OZ contained a similar provision on the general preventive duty.⁵⁰⁹ The case law on that provision may provide insights into the application of the new provision. Considering the difference in wording of the old and new provisions, it is not certain that older case law will still be followed. In any case, there is little to suggest that a more extensive interpretation of this duty will take place. If anything, the new wording seems more restrictive by limiting the general preventive duty to situations in which its application is required by the circumstances of the case and customs of private life, a condition that was absent in the old provision.

The general preventive duty was one of the most important provisions of the 1964 OZ and was frequently applied in later decades. It was used to establish the most extensive interpretation of the *neminem laedere* principle and encompassed not only damages directly caused by the obliged party, but also subsequent damages caused by other parties that can be related to the obliged party. The provision was motivated by the needs of the socialist society to strengthen socialist relations. The manner in which the preventive obligation was interpreted has been criticized as too extensive and as bringing legal uncertainty to civil relations.⁵¹⁰ Others point out that the strong emphasis on preventive duties stems from the fact that no compensation can fully restore the state of affairs before the wrongful act occurred.⁵¹¹

The new codification explicitly aimed to limit the application of the general preventive duty. The explanatory report states that cases in which the damage is caused by the party itself should be distinguished from other cases. The preventive duty should also be limited to what can be expected of a reasonable person according to the customs of private life, by the level of foreseeable responsibility connected to a certain behaviour, by the importance of the interest that the acting party pursues, by the nature of the relation between the parties, and by the accessibility and cost of the preventive measures.⁵¹²

⁵⁰⁸ Fekete 2011: 1027.

⁵⁰⁹ § 415 1964 OZ.

⁵¹⁰ Explanatory report to § 2900 and § 2901 NOZ.

⁵¹¹ Fekete 2011: 1026.

⁵¹² Explanatory report to the par. 2900 NOZ.

In Hradek's opinion,⁵¹³ the limitation of the preventive duty to the particular circumstances of the case and customs of private life will change the interpretation of the duty. While it was previously used to create new protective norms, the courts should now only apply existing duties. For instance, the current preventive duty cannot oblige a cyclist to wear a helmet if special laws only require this for cyclists of a certain age.⁵¹⁴ The courts did establish more extensive duties on the basis of the old general preventive duty.⁵¹⁵

While the recent legislative change was meant to reform the preventive duty, it is yet to be seen how the courts will interpret it. The available case law might not reflect the current state of positive law; nevertheless, a few important cases will be mentioned here.

The Supreme Court recently clarified that the general preventive duty is not boundless: everyone is obliged to show only the care which is reasonably expected in relation to the specific spatial and temporal circumstances and which is capable of preventing or at least minimizing the occurrence of damage. The provision does not establish a duty to foresee all possible future occurrences of damage.⁵¹⁶

Another insightful decision of the Supreme Court regards the question whether the general preventive duty can be breached in relation to one's own damage. In other words, what are the consequences for the damaged party who increased the likelihood or the seriousness of her own damage by her own careless conduct? The Supreme Court repeatedly ruled that careless conduct of the damaged party which increases the amount of damage is also a breach of the general preventive duty.⁵¹⁷ Based on this judgment, it may be reasonably expected that a computer owner who leaves her computer completely unprotected, for example by disabling the antivirus program and the firewall, would be found in breach of the general preventive duty and share at least part of the liability with the perpetrator if her computer is subsequently infected with malware.⁵¹⁸ In other words, what in other legal systems is called contributory negligence is determined by the same provision which establishes the negligence of other parties.

Several judgments clarify that the general preventive duty is not strictly limited to one's own actions, but can also arise in relation to the actions of other people. A driver of a car is obliged to ensure that the vehicle's other passengers do not endanger the safety of

⁵¹³ Hradek 2014, in Svestka, Dvorak, Fiala, (VI) 2014: 892.

⁵¹⁴ Svestka et al. 2013-VI: 892.

⁵¹⁵ See judgment 25 Cdo 2258/2008.

⁵¹⁶ Decision of the High Court in Prague from 4 February 2014 (preventive duty, liability) 1 Cmo 303/2013-166, commentary of Jaromir Jirsa 2014.

⁵¹⁷ Decision of the Supreme Court in Prague from 11 October 2006, sp. zn. 25 Cdo 1369/2006.
Decision of the Supreme Court in Prague from 27 June 2007, sp. zn. 25 Cdo 1448/2006.

⁵¹⁸ Tichy 2004: 47.

traffic, otherwise she is jointly liable for the damage caused.⁵¹⁹ A burglar who breaks into a house and leaves it vulnerable is also liable for damage caused by other thieves who take advantage of this vulnerability.⁵²⁰ An owner of a water slide is responsible for ensuring the safety of the slide and conducting oversight to ensure that it is used properly, otherwise she may be liable for damage caused by the unsafe behaviour of other persons on the slide.⁵²¹ By analogy, ISPs could perhaps be held responsible for cyber-attacks using their infrastructure, although their liability is limited by law (see section 5.5.1.3.1).

While the general preventive duty requires careful action of everyone, the special preventive duty (§2901) obliges certain subjects not only to act with reasonable care, but also to actively intervene to prevent damage that is about to occur to another person. This duty applies to those who create a dangerous situation or have control over it, or if the relation between the persons requires it. This duty binds every person with the possibility and the ability to prevent damage and who is aware or should be aware that the potential damage is clearly more serious than the effort needed to prevent it. The duty to actively intervene to protect a third person is an innovation of the NOZ. The 1964 OZ only obliged subjects to protect themselves.⁵²²

The duty to actively prevent damage requires a genuine and present threat of damage, not just a vague fear of potential danger.⁵²³ We can speculate that if, for example, a software vendor knows of a serious bug in one of its software programs which can potentially cause damage to users, it has a duty to intervene and undertake steps to prevent such immediately present danger, at least by informing the users about such danger. However, if the vendor only has doubts about the product, but no specific knowledge of dangerous bugs, or if the known bugs are not particularly dangerous, the duty does not materialize.

The relation between persons that establishes a duty to act to prevent damage to the other person is usually understood as a contractual or pre-contractual relationship. However, in some cases even ordinary social contact of people can establish such duty.⁵²⁴ Contractual relations generally establish a higher standard of care.

The duty to act is limited by the degree of danger and costs of such intervention. A person is only obliged to act if the danger she prevents is significantly larger than the danger this person would put herself in. If the prevented damage is smaller than the costs of preventive action, the person does not have a duty to act. This difference between the danger or damage prevented and the costs of preventing it should be clear. A minor or

⁵¹⁹ Fekete 2011: 1029.

⁵²⁰ Fekete 2011: 1031.

⁵²¹ Fekete 2011: 1032.

⁵²² Svestka et al. 2013-VI: 897.

⁵²³ Svestka et al. 2013-VI: 898.

⁵²⁴ Svestka et al. 2013-VI: 898.

arguable difference does not suffice to establish duty to act.⁵²⁵

Other preventive duties in the NOZ include the duty of a person who is in breach of her legal duty or knows that she will be in such breach to inform without undue delay any person that might be damaged by such breach of a legal duty,⁵²⁶ and the duty of a party who is at risk of being damaged to intervene in a proper manner in order to avert this danger.⁵²⁷

The costs of any preventive action taken in favour of another party are to be reimbursed, unless the action is taken to prevent a dangerous situation which was brought about by the actor herself.⁵²⁸ This provision can potentially support and motivate subjects to fulfil their statutory preventive duties.

5.5.1.2. *The regimes of liability under Czech law*

The NOZ knows three general grounds of liability:

1. Liability arising from a breach of *boni mores* (dobré mravy)⁵²⁹
2. Liability arising from a breach of a statutory duty⁵³⁰ (including general and special preventive duties)
3. Liability arising from contract⁵³¹

Ad 1. The Constitutional Court defined *boni mores* as an aggregate of ethical principles which are generally accepted and adhered to and which are often enforced by legal norms to ensure that all conduct complies with the general moral principles of democratic society. Furthermore, the concept of *boni mores* develops in time and space and has to be determined in the context of a particular case.⁵³² It is also defined as an unchallengeable mini-

⁵²⁵ Svestka et al. 2013-VI: 898-899.

⁵²⁶ § 2902 NOZ.

⁵²⁷ § 2903 NOZ.

⁵²⁸ § 2908 NOZ.

⁵²⁹ § 2909 NOZ: "Škůdce, který poškozenému způsobí škodu úmyslným porušením dobrých mravů, je povinen ji nahradit; vykonával-li však své právo, je škůdce povinen škodu nahradit, jen sledoval-li jako hlavní účel poškození jiného.

⁵³⁰ § 2910 NOZ: "Škůdce, který vlastním zaviněním poruší povinnost stanovenou zákonem a zasáhne tak do absolutního práva poškozeného, nahradí poškozenému, co tím způsobil. Povinnost k náhradě vznikne i škůdci, který zasáhne do jiného práva poškozeného zaviněným porušením zákonné povinnosti stanovené na ochranu takového práva.

⁵³¹ § 2913 NOZ: "(1) Porušil-li strana povinnost ze smlouvy, nahradí škodu z toho vzniklou druhé straně nebo i osobě, jejímuž zájmu mělo splnění ujednané povinnosti zjevně sloužit.
(2) Povinnosti k náhradě se škůdce zproští, prokáže-li, že mu ve splnění povinnosti ze smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním smlouvené povinnosti v prodlení, ani překážka, kterou byl škůdce podle smlouvy povinen překonat, ho však povinnosti k náhradě nezproští."

⁵³² Kamila Bubelova 2010: 3

mum standard of decency of all righteous persons.⁵³³ At first glance, the concept seems to hold some potential for the courts to establish something like a duty to care, built on the ethical norms in the society. However, only an intentional breach of *boni mores* establishes grounds for liability.

Ad 2. The following conditions establish statutory liability under Czech civil law:

- A person caused damage to another person.
- The damage is caused by a breach of a statutory obligation. In case the damage is to absolute rights, any breach of any statutory obligation will establish liability. If relative rights are at stake, only a breach of a specific duty devised to protect these rights will have such effect.⁵³⁴
- Fault, which in case of a breach of statutory obligation is presumed to be negligence. A person can exculpate herself by proving that she did not act negligently. Gross negligence or intent must be proven by the claimant.⁵³⁵ In general, a person is considered to act negligently if she doesn't act according to what can be reasonably expected in private matters from an average person. That a person has the mind of an average man and the capability to use it with usual care and caution is generally presumed by Czech civil law.⁵³⁶ However, what is considered to be an average mind depends on the particular group or profession that a person belongs to,⁵³⁷ e.g. a system administrator is expected to have the mind of an average system administrator. Therefore, if a person proclaims to have a special skill, knowledge or care, or promises to perform an action which requires such special skill, knowledge or care, and does not use such special attributes, it is presumed that she acts negligently.⁵³⁸ Professionals such as network administrators are therefore required to comply with a higher standard of care than non-professionals. Fault is not required to establish liability in specific cases provided by the law: in these cases, objective responsibility arises.⁵³⁹

Ad 3. Liability can also arise from a breach of contract. This type of liability only binds the contractual party that is in breach of the contract against the other contractual party or a person in whose benefit the contract was clearly concluded,⁵⁴⁰ although past case law has

533 Svestka et al. 2013-VI: 923.

534 Svestka et al. 2013-VI: 930.

535 Svestka et al. 2013-VI: 941.

536 Svestka et al. 2013-I: 30.

537 Svestka et al. 2013-VI: 951.

538 § 2910-2912 NOZ.

539 Svestka et al. 2013-VI: 877.

540 § 2913 NOZ.

extended this liability somewhat further.⁵⁴¹ Contractual liability is an objective liability and the party that is in breach of contract can be relieved of her liability only if she can prove that performance of the contract was prevented by a temporary or permanent, exceptional, unpredictable and impassable obstacle which has arisen independently of her will. This exception to liability cannot be applied if the obstacle arose from the personal situation of the party who is in breach, or if it arose at a time when performance should have already occurred. A contract can also specify that the party is obliged to overcome certain obstacles, in which case the liability will not be limited by the existence of such obstacle.⁵⁴² The contractual party can also be in breach in case the damage is caused primarily by actions of third-parties,⁵⁴³ if she was under a contractual duty to protect the other party from such actions.

Besides the three general types of liability, the NOZ recognizes a number of special liability regimes. Of these only one seems to have any relevance to this report: the liability for damages caused by a faulty product, which could theoretically come into play with regard to e.g. hardware or software manufacturers or vendors.⁵⁴⁴ This special liability was introduced to Czech civil law by the transposition of Council Directive 85/374/EEC.⁵⁴⁵ The liability for a faulty product lies with the manufacturer or the person that marked the product with their name or by other means, or with the supplier. If the product is imported, the liability lies with the supplier, even if the manufacturer is known. The product is considered faulty when it is not as safe as it can reasonably be expected to be with regard to all circumstances, especially the way in which it is introduced to and propagated on the market, the purpose it serves and the time in which it was introduced. The safety of the product is generally understood in terms of the consumers' health,⁵⁴⁶ however, a broader understanding of safety should not be refused out of hand. The liability for a faulty product is a type of objective liability, although certain facts mitigate the liability of the manufacturer or the supplier; such facts exist in particular if the fault of the product is caused by the damaged party, if the fault did not exist at the time of introduction of the product on the market, or if the state of technical and scientific knowledge at the time of its introduction did not allow the fault to

541 On the basis of the old Civil Law the Supreme Court ruled that the party in breach of contract not is only liable for the damage caused to the other party of the contract, or a subject in whose favor the contract was concluded, but also to such persons damaged by the breach of contract in whose legal sphere the obligation had an impact.

542 § 2913 NOZ.

543 NS 32 Odo 1180/2004.

544 See section on Software vendors for the discussion whether software can be considered a product for the purposes of this provision.

545 Svestka et al. 2013-VI: 1047.

546

be recognised.⁵⁴⁷ An important note to make here is that the provisions on liability for faulty products only protect consumers, not actors pursuing their commercial activities.⁵⁴⁸

5.5.1.3. *Liability of particular types of subjects*

5.5.1.3.1. *ISPs*

ISPs are subject to the general legal rules applicable to all legal subjects.⁵⁴⁹ Moreover, specific rules establish a separate regime for ISPs, regarding in particular their liability for the information they transmit or store. Next to these specific rules, certain principles restrict the scope of actions that ISPs can take (as an obligation or voluntarily) to prevent cybercrime. These include i.a. the protection of privacy enshrined in the Bill of Fundamental Rights and Freedoms,⁵⁵⁰ the principle of net neutrality that is promoted by the Czech Telecommunications Bureau,⁵⁵¹ and the ‘right to internet access’ which has been affirmed by the Czech Constitutional Court.⁵⁵² Potential preventive actions of ISPs, such as inspection of data, the blocking of websites and services, or the blocking particular users might violate these principles and therefore be in violation of the law.

Radim Polčák briefly sketches a few arguments for and against holding the ISPs liable for third-party content or information. An argument in favour of liability is that ISPs provide the infrastructure for disseminating such information and derive profit from this. Excluding their liability would put them in a privileged position compared to other parties. Additionally, even if they were held liable, they could in turn claim damages from the originator of the information. However, there are strong arguments against liability of ISPs. First of all, the traffic that ISPs transmit through their infrastructure is enormous and any of it could potentially be illegal. Secondly, the ISP may provide the infrastructure used for an illegal activity, but the importance of a particular informational connection for the ISP is negligible. The profit that it gains from a single connection is marginal, even though the damage such connection can cause may be significant. Thirdly, the services are often provided anonymously and it would often be practically impossible for the ISP to identify the originator of the illegal content and claim a regressive compensation. It is therefore clear that establishing objective responsibility of ISPs would require them to actively monitor all the traffic flowing through their infrastructure, which would not only pose practical difficulties, but also cause

⁵⁴⁷ § 2939-2943 NOZ.

⁵⁴⁸ Svestka et al. 2013-VI: 1064.

⁵⁴⁹ Polcak 2007: 51.

⁵⁵⁰ Art. 7(1), 10(2), 13 of the Bill of Fundamental Rights and Freedoms (Listina základních práv a svobod).

⁵⁵¹ See: http://www.ctu.cz/cs/download/obecna_pravidla_a_doporuceni_pro_vyuzivani_rizeni_datoveho_provozu_19122013.pdf

⁵⁵² I.ÚS 22/10 from 7. 4. 2010.

numerous issues, including infringements of privacy and data protection.⁵⁵³

The arguments against full liability of ISPs have prevailed. Under Czech law, all ISPs are excluded from objective liability, meaning that they are never liable for illegal communications of which they are not aware.⁵⁵⁴ This was established by statute 480/2004 coll. on selected services of information society. Prior to this piece of legislation, the liability of ISPs was not regulated; it was usually governed by an agreement with the user, which was problematic because the contract law at the time did not allow for the exclusion of liability for illegal acts. At that time, the general preventive duty (see section 5.5.1.1) would apply to ISPs, whose liability in such a case was secondary to the actual perpetrator.⁵⁵⁵ However, there is no case law about ISP liability under the general preventive duty according to the available sources. In any case, the new statute limits ISP liability to such an extent that the general preventive duty may not have any additional application.

The Czech law (statute 480/2004 coll. on selected services of information society) distinguishes three main types of ISPs and attaches to each a different regime of liability. The law was adopted as a Czech transposition of Directive no. 2000/31/ES, although the negative specification of ISPs' liability is replaced by a positive specification in the Czech statute. The significance of this choice will be explained later.

The main types of ISPs distinguished by the law are:

- ISPs providing mere conduit, i.e. access providers. These ISPs enjoy the most extensive limitation of liability. They are only liable if the illegal information can be attributed to them, for example if it originates from them, i.e. they created or modified it. They are not liable for information which does not originate from them, even if they know about the illegal nature of such information.⁵⁵⁶ Their duty to care therefore lies only in making sure that they do not create and disseminate illegal information themselves. They are practically free from worry about private users making claims against them under the argument that their subjective rights are breached.⁵⁵⁷
- ISPs providing caching. The liability of these ISPs is limited in the same way as the liability of access providers, with the addition that they are also liable if they do not comply with technical standards, contractual technical conditions, or conditions that are generally complied with in the industry.⁵⁵⁸ These ISPs, therefore, have an additional duty to care that lies in ensuring that proper technical standards are followed.
- ISPs providing hosting services. These ISPs are, in addition to the above, also liable

⁵⁵³ Polcak 2007: 53-54.

⁵⁵⁴ Polcak 2007: 55.

⁵⁵⁵ Riha 2008: 120.

⁵⁵⁶ Riha 2008: 121.

⁵⁵⁷ Polcak 2012: 148.

⁵⁵⁸ §4 Statute 480/2004 coll.

when they should, considering the nature of their activity and the circumstances of the case, have knowledge of the illegality of any information stored or activity, or when they learn about the illegal nature of the stored information and they do not immediately take steps to delete it.⁵⁵⁹ However, these ISPs are not obliged to actively monitor the content of information they store.⁵⁶⁰ Therefore, in practice, liability arises only if the ISP was properly informed about the illegal nature of such information. These rules might discourage ISPs from monitoring for dangerous information. If ignorance means no liability, there is little motivation for the ISPs to actively uncover illegal activities because by learning about it, they become liable if they do not immediately take action.

There are few court cases that could help in understanding how this framework is used in practice. Cases relating to a duty of the hosting ISP to remove illegal posts from discussion forums (defamatory parts) are available, however, to our knowledge, cases relating to cybercrime are not available. The literature is critical of the legislator's choice of wording of the provisions limiting liability of ISPs.⁵⁶¹ The provisions originate from Directive 2000/31/EC, which negatively limits the liability of ISP: ISPs are not liable in case of x (exceptions to liability). The Czech law is formulated positively: the ISP is only liable in case of x (cases in which the ISP is liable).

The significance of this difference is that while the Directive intended to establish exceptions to liability rather than separate grounds for liability, meaning that even if none of the exceptions apply, the ISP is not necessarily liable. Liability has to be derived from other legal norms, such as the NOZ. Czech law, however, seems to establish separate and exclusive grounds for the liability of ISPs. According to Polčák, the provisions of statute 480/2004 coll. should work only as a subsidiary norm limiting liability. However, their wording seems to confuse courts,⁵⁶² which apply the provisions as if they establish separate grounds of liability.⁵⁶³ The danger of such wording is that it does not seem to allow for any other grounds for liability of ISPs other than those specifically mentioned in the statute, which risks that the law will not adequately cover unpredictable cases.⁵⁶⁴

In conclusion: Czech law presently does not impose a general duty of care on ISPs to take action to prevent cybercrime. Although, a recent judgment,⁵⁶⁵ similar to the *Delfi v. Estonia* ECtHR decision, suggests that Czech courts are becoming more open to specifically talk about preventive duties of the ISPs, the decision is not final and remains isolated. As

559 §5 Statute 480/2004 coll.

560 §6 Statute 480/2004 coll.

561 Polcak 2012: 150; Riha 2008: 125.

562 E.g. judgment of the High Court in Prague from 2.3.2011 c.j. 3 Cmo 197/2010-82.

563 Polcak 2012: 150.

564 Riha 2008: 125.

565 66C 143/2013 – 510.

the law stands, only when an ISP has been informed about malicious information or content may the ISP be held to take action to remove such information or content. A particular duty that the ISPs *do* have under the Electronic Communications Act is a duty to collect traffic data and store it for a period of 6 months for the purposes of law enforcement.⁵⁶⁶

Finally, the fact that no specific statutory duty exists does not mean that certain duties of care cannot be contractually agreed upon between the ISP and its client. The contractual parties are free, within the limits of the law, to decide on the content of their contractual relations.⁵⁶⁷ If the client requires the ISP to take up some protective duties, it is entirely plausible that the ISP *would* take up such duties given the right incentives.

5.5.1.3.2. *Software vendors*

This section discusses the liability of software vendors for faulty products – that is, software that does not work as advertised or contains bugs which render it insecure and prone to cyber-attacks. In his book on software law, Jansa raises the concern that, considering the rapid development of the field, the Czech statutory law does not provide a sufficient regulation of it, while case law about software is negligible.⁵⁶⁸ Furthermore, most of the literature on software law in the Czech Republic focuses on the intellectual property aspects of software protection rather than the liability of software vendors or their responsibility for secure software.⁵⁶⁹

As specific regulation is lacking and general legal norms can hardly be applied in such a specialized field, the relations will largely be regulated by contracts.⁵⁷⁰ The application of general civil law rules in the field of software seems impractical: these rules in principle expect fulfilment of obligations without faults, which is practically impossible in contemporary software development.⁵⁷¹

This report is not extensive enough to contain an explanation on which subjects will be liable for defects in the software. Jansa and Otevrele describe six basic models of software distribution, explaining which subject (manufacturer, distributor, vendor) is liable under each model.⁵⁷² For the purposes of this report we will discuss the liability of software vendors, even though the same liability may under a certain distribution model apply to the manufacturer or distributor.

An assessment of the liability of software vendors under the regime of liability for

⁵⁶⁶ § 97(3) of the statute 127/2005 coll. The Electronic Communications Statute.

⁵⁶⁷ § 1725 NOZ.

⁵⁶⁸ Jansa, Otevrele 2014: 27-28.

⁵⁶⁹ E.g. Maisner 2011, Jansa, Otevrele 2014.

⁵⁷⁰ Maisner 2011: 80.

⁵⁷¹ Maisner 2011: 153.

⁵⁷² Jansa, Otevrele 2014: 147-151.

faulty products requires the determination whether software is a thing under the NOZ. The same question was raised by Jan Tomisek, who recognized that the absence of judicial guidance on this question as well as the lack of doctrinal answers prevented him from doing anything beyond arguing for his own opinion.⁵⁷³ He notes the possibility that the software license can be considered an immaterial thing since it fulfils the legal definition: it is separate from a person, serves the needs of people and can be the object of subjective property rights. Accepting this conclusion would entail that software has to be provided without faults⁵⁷⁴ if, in accordance with §1914 of the NOZ, the software has been provided in return for compensation, which could exclude free-of-charge software.

In general, the liability for defects in software will depend on contractual provisions. As the general types of contracts regulated in the NOZ are not applicable in the field of software law,⁵⁷⁵ software is generally governed by custom-made contracts. As a result, software is considered faulty when it does not correspond to what was agreed upon in the contract.⁵⁷⁶ The software should not only possess the attributes explicitly described in the contract, but also attributes which are standard for the type of software at hand. The purpose of the software is crucial in determining whether an attribute is standard, and thus whether the product is faulty.⁵⁷⁷ With regards to security and protection against cyber-attacks, the liability for an antivirus program is likely more readily established than liability for software which serves purposes unrelated to security. Furthermore, software vendors generally do not guarantee the absence of vulnerabilities, which also seems to preclude liability on the basis of a lack of care to avoid such bugs. This might be different if a vulnerability is proven to have been caused by gross negligence.

A general rule in Czech civil law, which will apply in the field software distribution, is that higher standards are expected of business entities and higher protection is attributed to consumers.⁵⁷⁸ If someone declares to have expert knowledge, a corresponding expertly care can be reasonably expected.

The lack of liability for vulnerabilities is further made possible by the fact that the NOZ, as opposed to the old ones, does not contain strict limitations on waivers of liability.⁵⁷⁹ In practice, software vendors often exclude liability for damage caused by third parties or by the proliferation of malware,⁵⁸⁰ and under the NOZ such liability waivers are much

573 Tomisek 2014: 34.

574 Tomisek 2014: 36-37.

575 Jansa, Otevrel 2014: 133.

576 Maisner 2011: 92.

577 Jansa, Otevrel 2014: 222.

578 Jansa, Otevrel 2014: 125.

579 Jansa, Otevrel 2014: 234.

580 Jansa, Otevrel 2014: 235.

more likely to hold up than before. It is often stipulated that free software is provided ‘as is’ (*jak je*), although this seems to be inadmissible.⁵⁸¹

As the duties of software vendors largely depend on the precise wording of the contracts, it seems plausible to conclude that they will only have limited duties to care: these contracts will most likely be drafted to limit or exclude their liability, especially in business relations. They may be held liable for breach of the preventive duties in case they fail to address known vulnerabilities of the software, but otherwise it cannot be reasonably expected of them to provide a completely bug-free software. With regards to damage to third parties caused in relation to vulnerabilities in their software, it seems unlikely that liability could be established considering an absence of contractual obligations towards these third parties and the general difficulty to prove the causality between the vulnerability and the damage.

5.5.1.3.3. *Businesses*

Businesses that are the victim of DDoS attacks may be in breach of their contractual obligations to provide a service (online). Whereas the contractual liability is an objective one and can be exculpated only if performance of the contract was prevented by a temporary or permanent, exceptional, unpredictable and impassable obstacle which has arisen independently of the obliged party’s will (5.5.1.2.), the determination of their liability to their customers will depend on their level of care to take precautionary measures to prevent any threats that could be predicted or overcome. The threat of failing to provide the service due to such attacks and being in breach of their contractual obligations may be an incentive to businesses to put proper precautionary measures in place. However, in practice it may be assumed that such contracts will often include clauses restricting liability. Other subjects may have a statutory duty to provide certain services online, but such breach requires fault to establish liability.

5.5.2. *Criminal Law*

In their criminal law textbook, Frantisek Novotny, Rudolf Vokoun and Pavel Samal write that computer related criminality is at the centre of public interest in the recent years.⁵⁸² This statement is not reflected in literature or case law, which are surprisingly scarce on this subject. Nevertheless, Czech criminal law has been recently recodified and includes several criminal offenses related to computers, networks and cyberspace.

The Czech Criminal Code (TZ) belongs to the continental legal system. A key feature of the TZ is its formalism – any behaviour that is not explicitly described in the TZ as a cri-

⁵⁸¹ Knebl 2010: available at: <http://pravniradce.ihned.cz/c1-46529960-odpovednost-za-vady-software>. [accessed: 6 February 2015].

⁵⁸² Novotny, Vokoun, Samal 2010: 209.

iminal offense cannot be criminally prosecuted and, at the same time, a behaviour that contains all the attributes of a particular crime is to be prosecuted regardless of other considerations.⁵⁸³ While the prevention of crime is one of the key functions of Czech criminal law,⁵⁸⁴ this does not entail that the TZ can be interpreted as containing extensive preventive duties subject to criminal sanctions. General principles of Czech criminal law include the principle of balance between public and private interest,⁵⁸⁵ the principle of *nullum crimen sine lege*,⁵⁸⁶ the subsidiarity of criminal repression,⁵⁸⁷ and the prohibition on the use of analogy against the interest of the offender.⁵⁸⁸ This set of principles entail that any criminally sanctioned behaviour has to be explicitly provided for in the TZ and that the provisions need to be interpreted rather narrowly.

In principle, for a certain behaviour to be qualified as a crime the Czech TZ requires this behaviour to be intentional. Only a limited number of crimes can be committed by negligence; namely if the TZ specifically mentions negligence. That said, the line between intent and negligence can be blurry in practice. Czech criminal law distinguishes between two types of intent as well as two types of negligence⁵⁸⁹ based on two categories of the perpetrator's psychological relationship to the crime (knowledge and will):⁵⁹⁰

- Direct intent: the perpetrator wants to damage or endanger the legally protected interest of society through conduct which is described by the TZ. In other words, she knows about the possible consequences of her action and wants them to occur. In general, direct intent is not a condition of criminal liability and indirect intent suffices, unless the description of the criminal behaviour contains wording such as 'with an aim' or 'intending'.⁵⁹¹ (knowledge and positive will)
- Indirect intent: the perpetrator knows that she can cause such damage or form a threat, and accepts this possibility. In other words, she has knowledge about the danger and is indifferent to the actual consequences. It is worth noting that the Supreme Court has

583 Herdova 2009: at: <http://www.epravo.cz/top/clanky/co-prinasi-novy-trestni-zakonik-55564.html>. [accessed: 5 December 2014].

584 Kratochvil 2012: 17.

585 Kratochvil 2012: 26.

586 Kratochvil 2012: 27.

587 Kratochvil 2012: 28.

588 Kratochvil 2012: 39.

589 § 15-19 TZ.

590 Kratochvil 2012: 280.

591 Kratochvil 2012: 288

interpreted indirect intent rather broadly in the past.⁵⁹² (knowledge and will that is neither positive nor negative)

- Conscious negligence: the perpetrator knows that the damage can occur, but without good reason expects it will not. As with both categories of intent, in this case the perpetrator has knowledge about the possible consequences of her actions; however, the difference is that she has a negative will towards the outcome. (knowledge and negative will)
- Unconscious negligence: the perpetrator does not know that her behaviour may cause the damage, even though she should or could have knowledge of it due to the circumstances and her personal situation. (no knowledge) The expected level of care required for an act to not be considered negligent is based on objective criteria of care (average person) or subjective criteria of care (based on specific attributes, standing and competence of the person).⁵⁹³ In principle, the same amount of care is expected of everyone, and only in exceptional circumstances (exercise of a profession) is a higher care expected.⁵⁹⁴

There is a fine line between indirect intent and conscious negligence. Even though it is clear that certain crimes require intent rather than negligence, in practice it may be less clear whether certain behaviour was intentional or negligent. The line is even more blurry in cases of gross negligence, which is a particularly serious case of conscious negligence and requires the perpetrator's attitude towards due care to indicate a serious contempt for the interests protected by law. Such serious contempt seems quite close to indifference, which is typical of indirect intent.

Another point to be made is that the person who directly commits the crime is not the only one who may be held criminally liable. The TZ recognizes several categories of aiding and abetting. A person who organizes or instigates the crime or a who helps the perpetrator to commit the crime is liable in the same way as the person who actually causes the damage. However, only *intentional* aiding establishes criminal liability.⁵⁹⁵ Alice Taborova opines that hosting ISPs may, under some circumstances, be criminally liable for aiding the primary criminal. This would in particular be the case if the ISP is aware of the illegal nature

592 NS(Rt) 11TDo 919/2004: "Fault in the form of indirect intent (...) can be assumed also in cases when the perpetrator intended another possible result, not important for criminal law, and the eventuality of the result described in the Criminal Code was unpleasant to him. If the perpetrator knew that as a result of his action the unpleasant result described in the Criminal Code can occur instead of the intended result, and did not count on any concrete facts which would prevent such development, and despite this acted, because he did not want to let go of such action even with the knowledge of the risk."

593 Kratochvil 2012: 293.

594 Samal 2012: 237.

595 § 23-24 TZ.

of the hosted information and does not act. In such a case, Taborova argues, indirect intent may be present, as is the required aid: the ISP provides the criminal with the space on the internet to commit the crime.⁵⁹⁶ A broad definition of aid is also presented by Vladimir Kratochvil, who defines aid as creating conditions which make the criminal behaviour easier than it would otherwise be. Such aid can consist of physical as well as psychological aid, and it can also be provided through omission.⁵⁹⁷ With regards to physical help, aiding can also consist of actions that are independent of the actions of the primary criminal, as long as the intent to aid her is present.⁵⁹⁸ The person providing such aid can exculpate herself if she voluntarily stops such aid and removes the danger, or notifies of the danger at a time when it is still possible to remove it.⁵⁹⁹

Omissions only establish criminal liability if there is a clear duty to act. Such a duty to act can be derived from a contract, from law, or, more specifically, from the position of guarantor.⁶⁰⁰ As described in the section on ISPs' liability, they only have a duty to act if they obtain knowledge about illegal information being hosted by them or if they are ordered to do so by a court, but they do not have an active duty to monitor for such information. Therefore, their criminal liability for omissions could only arise if they fail to fulfil the former duties.

There are several specific crimes relating to cybercrime. Hacking is criminalized in §230 of the TZ. It is interesting to note that accessing someone else's computer is only a crime if the perpetrator broke through security measures.⁶⁰¹ Therefore, a certain care of the victim is expected – if no security measures are in place on a computer, merely accessing it without permission is not a crime. However, accessing the computer and unauthorised interfering with the data in any way is a crime regardless of the security measures. Infecting the computer with malware, whether ransomware or for the purposes of DDoS attack, would therefore be a crime irrespective of whether the victim secured her computer. Because §230 requires intent it is unlikely that a third party, such as an ISP, could be complicit of the crime, for example by having lax security measures in place. In order to be complicit, the other party would have to be aware of an imminent attack and also of the potential con-

596 Taborova 2010: 49: In her paper, Alice Táborová writes favorably about the possibility of holding subjects such as the ISPs criminally liable (p. 45) – access providers for commissive action (p. 48), providers of caching services for both acting and omitting action that is required (p. 49), and host pro-viders for aiding the criminal by providing space on the internet (if they know about the illegal nature of the information hosted). However, Táborová stresses the importance of balancing the criminal re-sponsibility with the principle of subsidiarity of criminal repression.

597 Kratochvil 2012: 359.

598 Kratochvil 2012: 362.

599 Samal 2012: 353.

600 Riha 2008: 120.

601 Samal 2012: 2306-2307.

tribution of their conduct or omission to the attack, and be willing to take the risk. In such a case, indirect intent could be argued.

A related provision, §231, criminalizes the actions of someone who intentionally, for the purposes of hacking or intercepting communications, manufactures, imports, exports, sells, or offers (...) a device or its components, a manual, a tool or a program which serves to gain unauthorized access to an electronic communications network or a computer, or a password, entry code (...). This crime might be relevant especially in case of hardware or software producers and vendors. If they offer a product, a device or a program that could be used as a tool to gain unauthorized access to a computer, and they know that the person buying it will use it to commit such crime, then they could be held criminally liable. However, such liability would arise only, if the intended crime (hacking) wasn't committed. If it was committed, the vendor would be liable under §230 for aiding.

The third and last of the primarily computer-related crimes is the crime of damaging data on a computer or memory device or of negligent interference with a computer accessory.⁶⁰² Two things make this criminal offense very interesting for the purposes of this report. First, it does not require intent: gross negligence suffices for criminal liability. Secondly, resembling the German criminal law doctrine of *Garantenstellung*, to establish criminal liability, it is required that the perpetrator is in breach of a duty that stems from her work, profession, standing or function, or from statute or contract. It is, therefore, the specific aspect connected to the person that gives her extra responsibility and requires her to conduct herself with sufficient care, subject to criminal sanctions. If such a person acts or omits to act out of gross negligence and therewith causes data saved on a computer or a memory device to be destroyed, damaged, modified or made useless, or interferes with the technical computer accessories or with the software of a computer, and causes damage to someone else, she may face criminal sanctions - even though the same behaviour of an ordinary person, who is not in her position, would not be subject to criminal sanctions. The condition of gross negligence is fulfilled in particular if the person concerned repeatedly acts in a negligent way or was previously warned about such misconduct.⁶⁰³ The duty that is not complied with does not have to be an important one,⁶⁰⁴ but the damage caused must be at least 500 000 Czech Crowns⁶⁰⁵ (appr. 18 000 EUR). In the context of this provision, it is worth noting the new Cybersecurity Act (see section 5.5.3.) which establishes clear and rather extensive duties to professionals responsible for critical information systems, and other obligations can be established by the National Security Authority based on this

602 § 232 TZ.

603 Maisner 2011: 153.

604 Novotny, Vokoun, Samal 2010: 215.

605 Samal 2012: 2324.

Act. Non-compliance with these duties resulting in significant damage can lead to criminal liability under §232 TZ.

Another crime which may be relevant is the unauthorized disposal of personal data, even if only negligently.⁶⁰⁶ Unauthorised disposal can take form of publicising, sharing, making accessible personal data, other processing or appropriating of such data. The crime only concerns data that was collected in the exercise of public authority, but it can be committed by anyone.⁶⁰⁷ While not directly connected to cybercrime, criminals can use knowledge of personal data to make potential victims more vulnerable to such attacks. The TZ also criminalizes the unauthorized interception of letters, voice or data messages (...), as well breach of the privacy of writings or of computer data (...) kept in private spaces.⁶⁰⁸ These crimes do, however, require intentional conduct.

The crimes that might be applicable to software or hardware suppliers include breach of economic competition rules⁶⁰⁹ and causing damage to consumers.⁶¹⁰ Intentional distorting methods of competition such as misleading advertisement or misleading labelling can be criminally prosecuted if significant damage is caused to consumers. Introducing products, services or other works while withholding information about known faults of such products can also be criminally prosecuted. Any action that can mislead the consumer with regard to the quality of the product or service is considered withholding information (e.g. failing to mention the absence of protection against electric shocks or misrepresentations about the results of product testing). For instance, a software producer who introduces an anti-virus program in the knowledge that there is a serious bug in the program which may be utilized by criminals, or who advertises anti-virus software which is incapable of stopping most well-known malware, might be held criminally liable.

Furthermore, the Czech TZ includes two crimes that put certain responsibilities of crime-prevention and crime-reporting on every citizen. The two provisions, not preventing a crime (§367) and not reporting a crime (§368), both include an exhaustive list of crimes that everyone who has knowledge of their occurrence is obliged to report or make an effort to prevent. However, none of the crimes identified in the previous text as covering the field of cybercrime is included in these lists, which clearly indicates that citizens are not criminally liable for not preventing the actions of cybercriminals.

Overall, it seems like the potential of Czech criminal law to assume enforceable duties to care to prevent cybercrime is limited. Professionals working with computers (§232)

606 § 180 TZ.

607 Novotny, Vokoun, Samal 2010: 104.

608 § 182-183 TZ.

609 § 248 TZ

610 § 253 TZ.

and people in possession of personal data (§180) may be held liable for negligent actions. Hardware and software providers might be held liable for harming customers under §253. Otherwise, only subjects (1) with knowledge about the crime, and (2) positively disposed or indifferent towards it can be held liable for criminal offenses.

5.5.3. *Administrative Law*

A recent addition to the Czech legislative environment is the new Cybersecurity Act (Statute no. 181/2014 coll.). The law entered into force in January 2015. The goal of the new law is to establish a comprehensive approach to the cybersecurity of the Czech state, amid a growing concern on the dangers posed to the state by cyberterrorism. Cyberterrorism has already impacted some countries in the region, one example being the massive attack on Estonian cyberspace in 2007, during which the websites of banks, public institutions, ministries and the media were paralyzed by massive DDoS attacks.⁶¹¹ To protect the Czech cyberspace the new law puts in place a system of security standards for the information systems that are essential to the security and public order in the state.⁶¹² Many of these critical elements are not controlled by the state, but the new law establishes lines of legal action for those who do not comply with the security standards. These standards would also be reviewed through compliance audits of all public administration bodies and private parties controlling critical infrastructure. Formally, these functions are to be realised by the National Cyber Security Centre (Národní centrum kybernetické bezpečnosti) which is an organisational part of the National Security Authority (Národní bezpečnostní úřad) and which operates the Computer Emergency Response Team (GovCERT). The task of the GovCERT should not only be to react to existing incidents, but should also focus heavily on prevention and on the suggestion of measures to avert or thwart such attacks.

The new cybersecurity law establishes obligations for various subjects, including providers of electronic communications services, subjects who secure electronic communication networks, institutions or persons managing critical networks, administrators of the systems of critical infrastructure and administrators of its communication system, and administrators of important information systems. Their duties lie mainly in putting in place security standards which consist of organizational measures and technical measures. Examples of organizational measures include risk management, supply chain security, security of human resources, and control and audit of information systems. Examples of technical measures include physical security, tools to confirm the identity of users, and tools to protect against harmful codes and cryptographic tools. The extent of these duties is

611 Guardian: Russia accused of unleashing Cyber-war to disable Estonia. 17 May 2007: available at: <http://www.theguardian.com/world/2007/may/17/topstories3.russia>. [accessed: 5 December 2014].

612 The list of these information systems is maintained by the Government.

specified in government regulation (Notice 316/2014 Sb.).⁶¹³ Other duties include an obligation to report security incidents and to keep records about such incidents. These duties may be considered public law reflections of duties of care and diligence. Insofar as relevant, this shows that businesses and ISPs do, to a certain extent, have a duty to act to prevent cybercrime, although the extent of these duties appears to be limited.

The new law is seen as a big step forward in securing the cyberspace of the Czech Republic. Even though it is limited in scope, as it only covers the infrastructure critical for the exercise of public authority, in this limited sphere it establishes detailed and enforceable obligations aimed at the prevention of cybercrime. It may not offer much protection against malware such as ransomware to individual users, but it could be an important addition to the fight against DDoS attacks, which, after all, very often targets the critical infrastructure covered by the new law.

5.5.4. Conclusion

Czech law follows European Union rules as regards ISP immunity for liability, although choosing a different wording. Hence no general duty of care exists, even though a contractual duty can be agreed upon for customers of the ISP. Software vendors will not be liable if the contractual provisions are sufficiently limited, which they usually are. Hence there are only limited duties of care. Furthermore limitations clauses are allowed, albeit to a lesser extent than in the U.S.A. and The Netherlands. For businesses the same considerations apply: although a contractual duty of care and diligence may exist, actual liability will mostly be very much limited. There is no criminal liability for actors who unintentionally contribute to cybercrime. Noteworthy is only the possibility of criminal liability of software vendors for causing damage to consumers (§ 253 TZ). In particular cases this might form the basis for holding software vendors liable for vulnerabilities. The new Cybersecurity act does provide administrative law rules that can be viewed as laying down particular duties of care and diligence.

5.6. Conclusion

Although the jurisdictions investigated here do to a certain extent recognise duties of care and diligence that may counteract cybercrime, these duties have limited effectiveness.

ISPs may be contractually obliged to a minimal diligence for security measures and preventive action, but this diligence is hard to translate into obligations for specific actions. Furthermore, their clients may be unable to claim significant damages, due to contractual

613 Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.
Available at: <http://www.zakonyprolidi.cz/cs/2014-316>.

restrictions such as limitation clauses. ISPs are generally not liable towards third parties as long as they remain passive towards the information they transmit. This exemption rule actually provides an incentive for ISPs not to monitor for suspicious traffic. The U.S. rule that ISPs do not lose their immunity merely because of good faith efforts to monitor for certain types of harmful content is an exception. It should furthermore be noted that, although administrative law to some extent requires ISPs to help to prevent cybercrime, other rules and principles, such as the principle of net neutrality, actually prohibit preventive action or at least disincentivise actions such as discriminating between criminal communication and regular traffic. Administrative rules are however, relatively scarce and abstract in most of the jurisdictions studied; The Netherlands is an exception in having a highly detailed set of rules regarding ISPs. Regardless of the legal rules, there are indications that ISPs voluntarily take preventive action. This is understandable as ISPs themselves endure negative consequences from the prevalence of cybercrime.

Software vendors may, depending on the interpretation of the relevant contracts, have a duty of diligence to provide secure software. However, any such duty is usually made harmless by limiting the contractual warrants as regards the lack of security and by stipulating damage limitation clauses under which pure economic loss is not recoverable. Software vendors are not liable to third parties on the basis of negligence, except in special circumstances. The possibilities to hold a software vendor liable are even more limited if the software is provided for free. Product liability rules are not applicable to software, even though an analogous rule of liability for defects, with effective damages, might provide additional incentives for secure software. A notable exception is Brazil, where product liability rules do apply to software. Another exception is the possibility of criminal liability under Czech law for software or hardware that causes damage to consumers. The present economics of the software market provide disincentives against efforts to promote software security by prioritising the rapid marketing of functionality over careful development to avoid security leaks. It should be noted that there are no administrative rules regarding the software sector in general, in stark contrast with the position of ISPs, who are subject to administrative regulation.

Businesses that suffer from cybercrime (either because of malware present on their computers or by being the victim of a DDoS attack) may be required towards their customer to take actions. As regards the presence of malware: this may lead to the leaking of private data, which – given the data protection laws – is usually a breach of contract or a tort towards the individuals whose data is leaked. As regards defence against DDoS attack: such an attack causes the service to be unavailable to customers, which – depending on the kind of service and the contractual relation with the customers – may constitute a breach of contract. Liability, however, is usually limited due to limitation clauses or restrictive warranties.

Other actors, in particular those involved in the general Internet ecosystem (such as registrars, organisations responsible for the protocols and standards that constitute the Internet, or blacklisting organisations), may influence the ease with which cybercrime is conducted, but their actions and choices generally will not establish any liability towards victims of cybercrime.

6. Enforcement of duties of care and diligence

6.1. Introduction

The few duties of care and diligence identified in the previous paragraph do not appear very effective, as breach of these duties would only entail liability to a limited extent. The actual enforcement of these duties is even more limited, as will become clear in this paragraph. However, there are also other mechanisms that might induce compliance. These will be discussed in par. 6.6.

6.2. The Netherlands

As explained in par. 5.2, there currently are only limited obligations to take preventive measures against the forms of cybercrime discussed in this report. As regards enforcement of those obligations that do exist, the following applies.

6.2.1. Private law

Private law enforcement of the obligations discussed is primarily left to the initiative of the *individual victim*. Apart from the legal obstacles that may stand in the way of an individual claim, discussed in par. 5, it is generally not to be expected that individuals instigate civil proceedings against (for example) an ISP or software vendor on the ground of violation of a *zorgplicht*. The primary reason is that the damage suffered by individuals because of the kinds of cybercrime discussed here is usually negligible. Even in the case of ransomware criminals are not likely to ask too much money, as the victim might not be able to pay a too large amount., Bearing in mind the slim chances that such a claim is successful and the possibility of mitigation of damages due to contributory negligence on the side of the victim, the costs of starting civil proceedings⁶¹⁴ will generally be too high in relation to the possible award of damages. This might be different if the procedure would be accepted for subsidised financial support,⁶¹⁵ but even then a significant contribution is usually required of the individual, proportionate to income or assets.

For *individual businesses* the costs need not be a barrier, while the damage may be much larger, particularly in case of a DDoS attack. In this case, disincentives include complications in the area of proof of causality. The causes of a particular DDoS attack lie in a multitude of security breaches that lead to the infection of thousands of individual computers. It is next to impossible to prove which particular software vendors or ISPs have breached duties of care or diligence as a result of which the original causes – the infections – were able to take place. Once a botnet is in place, there are currently only limited possibilities to quickly dismantle or stop the botnet or block an attack. However, if the ISP with which the business has contracted for Internet services is able to limit the effects of the

⁶¹⁴ Which costs are not fully compensated even in case of a successful claim.

⁶¹⁵ Gefinancierde rechtsbijstand, funded legal aid.

botnet in some way and neglects to do so, a business might succeed with a claim.

In cases of manifest negligence on the side of a particular software vendor or ISP it might be an option to start a *collective action* to claim a correction of the deficient behaviour,⁶¹⁶ or to claim general damages on behalf of the victims. A claim for damages currently requires a mandate from the victim except if a collective settlement is reached and declared binding,⁶¹⁷ in which case the settlement may cover all victims who have suffered damage, regardless of whether they issued a mandate.⁶¹⁸ These mechanisms offer some room for interest groups to take the lead in enforcement of desirable behaviour. However, such groups are unlikely to start a procedure if there is no clear violation of a duty, particularly if there are no generally accepted standards. At present there appear to be no general interest groups that are active to promote higher security standards for ISPs and software vendors. On the contrary, the trend appears to be to instigate actions against stronger government monitoring of the Internet.

The possibilities for a civil action on the basis of art. 3:305a BW are also available to the government, including governmental authorities.⁶¹⁹ Whether they will do so will depend mostly on policy decisions which, given the limited time and funds available, are most likely influenced by considerations regarding cost, public interest, and the chance of success.

Insofar as a party does decide to start a procedure, Dutch law offers a variety of means for obtaining relevant evidentiary material. There are extensive information duties on the defendant,⁶²⁰ provisional witness hearings, possibilities for expert evidence, and statutory search orders (on the basis of art. 843a WBRv, comparable to the 'Anton Piller order'). Summary proceedings are available in urgent cases (art. 254 WBRv).

Dutch law offers several remedies: specific performance by an injunction or judicial order (strengthened with a penalty for non-compliance), award of damages, and a declaratory judgement. This allows a court to order, for example, that an ISP is to remove a website from its web server, to disallow certain specific data to be communicated, and to take certain safety measures. A court order should, however, not be too unspecific and should specify clearly the results required.⁶²¹

6.2.2. Criminal law

Enforcement of violations of criminal law is in the hands of the public prosecutor (*Officier*

616 Ordering an order of specific performance, on the basis of art. 3:305a BW.

617 On the basis of the WCAM (Dutch Collective Claim Act).

618 Except for the victims who expressly declared to opt out from the settlement.

619 Cf art. 3:305b and 2:1 BW.

620 Art. 19-22 Wetboek van Burgerlijke rechtsvordering (WBRv, Dutch Code of Civil procedure).

621 Although a court order to reach a certain result will be interpreted as that the defendant should make a best effort for that result.

van Justitie). The decision to start a criminal investigation and, subsequently, to start a criminal prosecution is based not only on whether there is sufficient evidence of a norm-violation, but also on expediency (*opportuiniteitsbeginnel*). There should be sufficient reason to prosecute this particular violation in preference to others, given the fact that there is not enough manpower available to follow up on all suspicions of criminal acts). In the case of duties of care and diligence to prevent cybercrime, the violation mostly consists of a failure to take action to prevent the actual criminal from achieving his aims. In general, there appears to be no urgent pressure to prosecute bystanders or non-complicit intermediaries or facilitators of the crime. However, duties of care and diligence to prevent cybercrime might be suitable in specific instances for giving a ‘signal’ that more cautious behaviour is actually required of ISPs and software vendors. As discussed in section 5.2.3, the Criminal Code seems to offer ground to prosecute in case of a clear failure to act, although it is uncertain whether the Hoge Raad would interpret the provisions of the Criminal Code sufficiently extensively.

Insofar as a decision is taken to investigate and prosecute, the police and prosecutor appear to have sufficient powers to obtain the necessary information and evidence for a case against the parties discussed in this report, at least at the national level. Obstacles arise in cross-border contexts, for instance where ISPs or vendors are located abroad while victimisation primarily takes place in the Netherlands, and where the principal perpetrators may be located in yet other countries. Mutual legal assistance procedures can assist to gather evidence in such cross-border cases (particularly among party states to the Cybercrime Convention). However, this requires dual criminality, so that it depends whether ISPs or vendors can also be prosecuted for breach of duties of care and diligence under the laws of the jurisdiction they are located in. Moreover, the success of mutual assistance will depend on the willingness of foreign law enforcement authorities to gather evidence and/or to take over prosecution, which may also be low if it concerns a prosecution of bystanders or non-complicit intermediaries rather than the perpetrators themselves.

6.2.3. Administrative law

As the failure to take action to prevent cybercrime may also constitute a violation of administrative law duties, various government agencies could be empowered to act against such violations. Given the principle of legality, such action must be based on specific legislative provisions that provide for specific sanctions, such as fines or the annulment of licenses. Administrative law could be a valuable supporting factor in state enforcement of desirable behaviour by giving supervisory authorities the power to sanction private parties, thereby providing targeted incentives for correct behaviour. A drawback is that the legality principle causes a delay in the response to new developments. The powers and sanctions generally have to be sufficiently specified, as a result of which constant updates in light of new forms

of undesirable behaviour may be required. Although Dutch administrative law does allow a certain amount of goal-directed regulation in the form of duties of care and diligence, there is strong doctrinal resistance against adopting this type of regulation.⁶²²

Enforcement of administrative obligations in telecommunications law is in the hands of the ACM⁶²³ and, as regards continuity the *Agentschap Telecom*, of the Ministry of Economic Affairs.⁶²⁴ In particular the ACM is fairly active in enforcing regulation applicable to ISPs. Failure to comply with the relevant administrative rules may also constitute an economic misdemeanour under the Economic Offences Act (*Wet op de economische delicten*),⁶²⁵ which could lead to criminal prosecution. However, this is rare.

6.3. U.S.A.

6.3.1. Private law

Regarding private law enforcement, individual victims may take action by starting a normal court procedure to claim damages.⁶²⁶ This course of action will normally be unfeasible for private individuals given the high costs involved, and may be impractical given the negligible damage they suffered. Businesses may have suffered significant losses and may have enough resources for legal proceedings to be economically feasible. However, private individuals and businesses alike will usually find themselves subject to exemption clauses which limit the possible award of damages to such a low amount that legal action is impractical. Injunctions usually will not offer much relief as most companies already provide updates to patch security vulnerabilities.

With regard to individual action against a software vendor, the problem is that it is hard to prove whether the loss is caused by the vulnerability. A later infection by malware need not be caused by one specific vulnerability. For victims of DDoS attacks, causality will be impossible to prove, as the botnet clients will in all probability have been installed through many different infection methods.

For collective action, the U.S. legal system has the class action.⁶²⁷ According to federal law, a class action may be started by at least one individual who is representative of the

622 See for example Hendrikse & Rinkes 2012 as regards a general duty of care for financial service providers, and earlier experiences with such duties for environmental protection.

623 Cf. Gijrath 2014: Ch. 3.

624 Art. 15.1 Tw, Art. 1(d) Besluit continuïteit openbare elektronische communicatienetwerken en -diensten of 19 October 2012, Stb. 2012, 514, art. 2(1) Besluit aanwijzing toezichthouders Telecommunicatiewet.

625 In particular violation of art. 11a.1 Tw, see art. 1(1) *Wet op de economische delicten*.

626 Generally about civil procedure: Farnsworth 2010, p. 109-110.

627 The federal class action is regulated in the Federal Rules of Civil Procedure, Rule 23, and Title 28 U.S.C. § 1332(d), 1453, and 1711–1715. The state of California has different rules for class actions.

whole class, i.e. who has been harmed by the alleged breach of contract or tort.⁶²⁸ Once the action has been certified as a class action, the court may – if it finds against the defendant – award damages for the whole class. Parties may also reach a settlement, although this requires the court's approval.⁶²⁹ The settlement then becomes binding for the whole class. Although a class action can be an effective means to provide incentives for businesses to comply with legal requirements towards consumers, in particular if individual damages are low, there is criticism too. Some settlements offer only very little compensation for individuals and some class action litigators display unethical behaviour.⁶³⁰ Class actions have been instigated in cases of loss of private data by companies like Sony and Dropbox.⁶³¹ That might provide an incentive to businesses to improve their security. Businesses may try to avoid the risk of class action by modifying their general terms and conditions or their terms of service to disallow class actions.⁶³² There are few class actions based on software vulnerabilities.⁶³³ The problem with such class actions appears to be that the mere existence of a vulnerability is not considered to be a breach, in particular if the vulnerability was not previously known by the vendor and if a patch was made available quickly.

6.3.2. Criminal law

The law of criminal procedure is largely found in the statutory law of states, showing considerable differences between the various states.⁶³⁴ The US District Attorney may decline or authorize prosecution in cases where there are arguably grounds for criminal prosecution.⁶³⁵ Given that there appears to be little ground to suppose that ISPs or software vendors who act in good faith (though somewhat negligently) are aiding and abetting cybercrime,

628 There are other requirements as well, see Rule 23 Federal Rules of Civil Procedure.

629 Rule 23(e) Federal Rules of Civil Procedure.

630 See Zitrin & Langford 1999.

631 For the Sony PSN security breach settlement see (<https://psnsoesettlement.com/>) for the Dropbox breach <http://dockets.justia.com/docket/california/candce/4:2011cv03092/242244>.

A list of technology related class actions suits, among which numerous data breach cases, can be found at <http://www.lawyersandsettlements.com/lawsuits-filed/internet-technology-lawsuits/>

632 For example <http://www.computerworld.com/article/2487987/cloud-computing/update--dropbox-changes-its-terms-of-service-to-stop-class-action-lawsuits.html>, choosing arbitration over court procedure and disallowing class actions.

633 Such as against HP for a printer software vulnerability (<https://techbuddha.wordpress.com/2011/12/08/class-action-lawsuit-against-hp-for-not-disclosing-security-vulnerabilities-has-huge-implications/>), against Samsung for a bug that freezes its mobile phones (<http://topclassactions.com/lawsuit-settlements/lawsuit-news/1966-samsung-galaxy-s-defect-class-action-lawsuit/>). The latter, however, appears not to be a pure software case as it involves hardware hence a product.

634 Farnsworth 2010, p. 122.

635 United States Attorneys' Manual (USAM) § 9-2.020 and 9-2.030.

it does not seem likely that the District Attorney will prosecute for breach of a duty of care and diligence.

As regards enforcement, criminal investigators can make use of a variety of instruments that oblige parties such as ISPs to cooperate, such as the Federal Wiretap Act, 18 U.S.C. §§ 2510-2522, the Stored Communications Act, 18 U.S.C. §§ 2701-2711, and the Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001 et. seq.⁶³⁶ A number of government agencies work towards combating cybercrime, including several divisions of the Department of Justice, and, regarding international cooperation efforts of the Department of State and the Department of Homeland Security. Also involved are the Private Office,⁶³⁷ the FBI and the CIA.⁶³⁸

6.3.3. *Administrative law*

As regards administrative law governing ISPs, the Federal Communications Commission (FCC) supervises and enforces the rules. The FCC is in charge of ensuring the efficiency of the U.S. communications network.⁶³⁹ It derives authority from Title 47 U.S.C., which places the FCC under an obligation to create 'regulations for common carriers, rules for interconnection between telecommunications carriers, rules to ensure 9-1-1 services, and regulations to promote diversity of information sources and services provided in cable communications'.⁶⁴⁰ Arguably the FCC may promulgate rules and standards regarding cybersecurity.⁶⁴¹

The Federal Trade Commission (FTC) does have some enforcement powers, but those do not relate to prevention of cybersecurity as such. The actions by the FTC in this respect mostly involve encouragement for action by other parties. There is dispute as to whether net neutrality would fall under the purview of the FTC.⁶⁴²

With regard to the enforcement of notification rules, this differs between various states.⁶⁴³

6.4. *Brazil*

The enforcement of duties of care and diligence in Brazil is primarily the responsibility of

⁶³⁶ Mehra 2010: 671-675.

⁶³⁷ Mehra (2010: 679-681), also mentioning Department of Commerce, National Telecommunications and Information Administration (NTIA) and United States Trade Representative, Office of Intellectual Property and Innovation. These agencies are however not relevant for the present research.

⁶³⁸ Deflem & Shutt 2012, p. 3.

⁶³⁹ Sherling 2014, p. 588. Referring to 47 U.S.C. § 151 (2006).

⁶⁴⁰ Sherling 2014: 587, also 570.

⁶⁴¹ As argued forcefully by Sherling 2014: 589ff.

⁶⁴² Boliek 2011.

⁶⁴³ Shaw 2010: 531-534 with details.

the victims, who can claim damages in an individual court procedure. If the case is based on the general law of obligations (contract law) or tort law, the victim has to prove causality and loss (Art. 333, I, of the Brazilian Code of Civil Procedure). Civil liability claims lapse after a period of three years (Art. 206, §3, V, BrCC). If the damage, however, is caused by a product or service in the framework of a consumer relation, the specific set of laws of the BrCDC comes into play. The inversion of the burden of proof is among the most important procedural aspects of consumer torts (Art. 6, VIII, BrCDC). The BrCDC establishes that the burden of proof is inversed in favour of the consumer in three specific situations, in which this prerogative emanates from the law and does not depend on evaluation by the court.⁶⁴⁴

First, in the case of defective products, the supplier will be liable for the damage claimed by the consumer unless he is able to prove one of the exceptions to liability listed in Art. 12, §3, BrCDC, namely: I - he did not place the product on the market; II – the product is not defective; III – the fault rests entirely with victim or a third party. In the absence of such proof, the court will recognize the elements of the tort to uphold the consumer claim. While the system is beneficial to the consumer – at least in theory –, the victim is still expected to present a reasonable and credible measurement of the material and possible moral, esthetical, or reputational damages. This can be particularly challenging in the context of cybercrime, as the individual damage caused to each affected user can be rather small.

Second, and similarly to defective products, the supplier of a defective service will be liable for the damages claimed by the consumer unless he can prove that the service is not defective or that the defect is the exclusive fault of the victim or of a third party (Art. 14, §3, BrCDC). Therefore, the consumer does not need to prove the defect of the product or service: it is for the supplier to rebut these claims.⁶⁴⁵

Third, it is for the supplier to prove that the information provided to the consumer or to ads and marketing services is accurate (Art. 38, BrCDC),

Consumer liability claims lapse after different terms. Noticeable vices prescribe after a term of 30 days for perishable products and services or after 90 days for non-perishable products and services, counting from the day on which the product or service was effectively delivered (Art. 26, I, II, BrCDC). The term for claims about hidden vices starts the day on which the vice became evident (Art. 26, §3, BrCDC). Finally, damage claims linked to defective products or services prescribe after a term of 5 years, counting from the moment in which the damage and its author became known (Art. 27, BrCDC).

Complaints for consumer torts can be filed by individuals or via collective actions

644 Tartuce, Flávio & Neves, Carlos. Manual de Direito do Consumidor. Direito Material e Processual. 3 Ed, Editora Método, São Paulo, 2014, p. 418

645 Tartuce, Flávio & Neves, Carlos. Manual de Direito do Consumidor. Direito Material e Processual. 3 Ed, Editora Método, São Paulo, 2014, p. 419

(class actions) (Art. 81, BrCDC, and Art. 1, II, Law 7.347/1985).⁶⁴⁶ Consumer class actions remove the financial burden from the consumer, as there is no advance payment of the procedural costs (including the costs of the claim, legal fees and expert expenses) and as the claiming association cannot be condemned to pay the other party's costs, except if it acted in bad faith (Art. 87, BrCDC). Nevertheless, class actions can only be initiated by a set of legitimate parties, as prescribed by Art. 5, of Law 7.347/1985.⁶⁴⁷ Only public prosecutors, public attorneys, entities of the Federal State, autarkies, foundations, state-owned companies, and civil society associations are authorized to bring consumer class actions to court. Individual consumers may decide to join the collective action, after which they can obtain an individual award of damages, but may also opt out of the claim.⁶⁴⁸ Although the legislator waived the procedural costs for collective actions and the Brazilian Federal Constitution grants possibilities of free access to justice (Art. 5, LXXIV), the procedural costs of individual claims are still a major impediment to access to justice, especially if the individual damages are difficult to assess, as in cases of reputational damage and data loss. The individual remedies available to consumers therefore seem to provide an ineffective means of enforcement

6.5. Czech Republic

This section will discuss the enforcement of duties of care and diligence in the Czech Republic that were identified in the previous chapter. The discussion is limited by the complete absence of case law related to the enforcement of such duties of care and diligence with regards to the three aspects of cybercrime discussed in this report. Given that case-law regarding such duties of care and diligence is absent (or at least could not be identified during the research for this project), the following analysis is not based on the enforcement as grounded in practice, but rather on the theoretical possibilities and barriers of enforcing duties of care and diligence.

Because many of the duties of care and diligence are established by contracts, especially in software law, it is crucial for their enforcement that the contracts are drafted clearly and properly. Martin Maisner mentions several problems of such contracts that arise in Czech practice: (1) unclear specification of the obligation (attributes of the program), (2) use of specialized terminology that is not clearly defined and is often interpreted differently by the parties, and (3) use of (improperly) translated English terminology that is not suitable

646 Official version available at http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm (in Portuguese)

647 Law of Public Civil Suit (Law No. 7.347/1985), see <http://www.processoscoletivos.net/brazilian-class-actions/1061-public-civil-suit-law-n-7-347-1985>, also <http://www.iclg.co.uk/practice-areas/product-liability/product-liability-2014/brazil>, par. 4.3.

648 Gidi 2003: 341. Also <http://thebrazilbusiness.com/article/class-action-class-suit-and-representative-action-in-brazil>.

ble in Czech legal system.⁶⁴⁹ These shortcomings hamper the enforcement of obligations in software contracts.

The Czech Code of Civil Procedure (OSŘ) gives the parties several tools to enforce obligations that others have towards them or to claim the compensation of damages caused by the breach of such obligations. A reconciliation procedure endorsed by the Court may under certain circumstances be used to reach a settlement. The Court can also decide to take a precautionary measure or secure evidence before the main proceedings. A party who claims that someone has an obligation (stemming from the law, a legal relation or a breach of law) towards her can file an action to perform the obligation. The claimant has to prove that the defendant is indeed subject to this obligation. In a claim for damages, the claimant has to prove the occurrence of the damage and the causal relation between the damage and the conduct of the defendant.⁶⁵⁰ Both parties have the option to appeal the judgment in the first instance and, in specific circumstances, also to appeal the decision of the appeal court. The length of proceedings can significantly hinder the enforcement of duties established by substantive law. The average length of civil proceedings differs per court, ranging from 122 days to 876 days, with 369 being the average in the Czech Republic.⁶⁵¹ Considering the added length of the appeal procedures,⁶⁵² the judicial delays and related costs of the proceedings can be a serious deterrent to anyone wishing to enforce such duties to care or diligence, especially since the state of substantive law makes it far from clear whether such duties actually exist or not.

These practical issues related to the cost and length of judicial procedures might be mitigated by the possibility to take collective action, under which a large number of victims act together. However, the option for collective actions is provided for only indirectly in §159a(2) of the OSŘ: the decision of the court in matters specified in §83(2) is not only binding for the parties of the hearing, but also for other persons having claims towards the defendant stemming from the same conduct or the same state of the affairs. This is of limited value since it only applies to a limited set of case scenarios and does not provide for true collective action.

Although an important tool of enforcement, lawsuits are not the only and perhaps not the most efficient way of enforcing duties to care. Often a simple notification of the relevant subject about ongoing illegal activity can lead to the solution. In fact, as mentioned in chapter 5, such notification can in certain cases establish to duty to act that did not exist previously.

649 Maisner 2011: 84-86.

650 Maisner 2011: 93.

651 Právní prostor. 28 November 2014: available at: <http://www.pravniprostor.cz/clanky/ostatni-pravo/novy-projekt-mapa-prutahu>. [accessed: 1 February 2015].

652 A table (updated as of 2011) of the average length of judicial procedures: [http://www.czso.cz/csu/2012edicniplan.nsf/t/9A002AD93B/\\$File/0001122702.xls](http://www.czso.cz/csu/2012edicniplan.nsf/t/9A002AD93B/$File/0001122702.xls) (Statistical Bureau of the Czech Republic).

In criminal law, enforcement problems have also been observed. While the public prosecutors are obliged by law to prosecute every crime that is made known to them,⁶⁵³ the law enforcement authorities might not have the capacity to properly investigate every incident of cybercrime. In practice, the norms of criminal procedure are not capable of keeping up with developments in the field and often hinder or slow down the law enforcement authorities. The procedures take too long and often a suitable procedure is missing altogether.⁶⁵⁴

The enforcement of rules about the prevention of cyber-attacks is especially problematic since the target of the crime, in contrast with the cybercriminal, cannot know when and how the attack will be executed. Nonetheless, Jakub Harašta is of the opinion that proper analyses of the risks and setup of security standards and policies can prevent a large portion of such attacks. In the Czech Republic, this role is currently fulfilled by the Strategy for the field of cybersecurity in the Czech Republic for the period of 2011-2015, which aims to create effective policies to strengthen the critical information systems, incorporate security standards and their control, detect dangers and devise solutions to minimize such dangers.⁶⁵⁵ Harašta also identifies a number of challenges of the implementation of cybersecurity project in the Czech Republic and the Central and Eastern European region in general: (a) rejection of control measures by the public (influenced by the recent experience with totalitarian regimes), (b) insufficient expertise of public officials, who are often selected for political reasons rather than competence, and (c) the problem of corruption that often delegitimizes the implementation of projects in the eyes of the public.⁶⁵⁶

Maisner is of the opinion that the public sector should cooperate more intensively with IT sector associations and, together with the private sector, build best practice systems. As an inspiration he mentions the UK's Nominet.⁶⁵⁷

653 § 2(3) Code of Criminal Procedure (TrŘ).

654 Taborova 2010: 44.

655 Harašta 2013: 80.

656 Harašta 2013: 86.

657 Maisner 2011: 279.

6.6. *Alternatives for compliance*

6.6.1. *Introduction*

The literature on alternative means of regulation (understood here as improving compliance) is vast and cannot be fully discussed here. However, a number of specific means and practices are relevant to the present topic. We will focus on those.

6.6.2. *Cybersecurity insurance*

One consequence of the rise of notification laws in the U.S.A. is the consequent rise of cybersecurity insurance.⁶⁵⁸ Insurance companies offer insurance against the risks associated with security breaches that have to be notified.⁶⁵⁹ This typically covers damage to digital assets, interruption of business, and possibly reputational damage.⁶⁶⁰ But the insurance policy may be more extensive by also providing coverage for the cost of notifying affected customers, IT defensive services, forensic investigation, legal advice and assistance, or public relation services. The policy may be to pay for these services, but the insurer may also suggest experienced service providers who are able to step in at short notice. Extended coverage is particularly useful for small and medium-sized businesses, which may not have the means to employ a specialised staff for such eventualities.

A beneficial effect of insurance is that the insurance company has an incentive to critically assess and reduce the risks of breach, and can – through the mechanisms of premium reduction and conditional performance in case of an actual breach – effectively and efficiently enforce risk-reducing measures. Because insurance companies with a sufficiently broad portfolio may obtain extensive experience with a wide variety of breaches, they may come to adopt and enforce an empirically grounded set of best practices to prevent and counteract security breaches, potentially reducing the number of such breaches.⁶⁶¹ The resulting improvement of compliance with the ultimate government goal of minimising security breaches is obtained with minimal supervisory cost to the government, as the costs are mostly borne by the companies which are open to such risks.

This phenomenon of regulation through notification may be applicable in specific other cases as well.

658 Constantin 2014, see also <http://www.dhs.gov/publication/cybersecurity-insurance>. Alternative names are Cyber Risk Insurance or Cyber Liability Insurance, cf. Cyber Liability Insurance Cover (Sembhi 2013).

659 Naturally the actual coverage may be broader.

660 Constantin 2014, see also Sembhi 2013.

661 The U.S. Department of Homeland Security is aware of this, see <http://www.dhs.gov/publication/cybersecurity-insurance>. See also positive: Peters 2014: 1199-1201.

6.6.3. *Self-regulation and soft law*

Even a brief survey conveys many examples of soft law initiatives to combat cybercrime. These are not binding, but they do give an impression of what non-obligatory actions are possible. Does soft law in this regard lead to more compliance? As pointed out above, business organisations may on occasion play a role in improving compliance as well. This is often discussed under the heading of self-regulation or soft law. Existing initiatives might have only limited effect on the topic at hand.⁶⁶²

ISPs. The United States Internet Industry Association (USIIA), in which ISPs are organised, has been concerned with cybercrime and has discussed self-regulation of the industry, but rejected any assumption of a legal obligation to police the Internet.⁶⁶³ For a long time, ISPs have been encouraged to take steps to combat botnets and malware.⁶⁶⁴ In March 2012, the Federal Communications Commission (FCC) similarly unveiled that a group of ISPs voluntarily adopted recommendations to address vulnerabilities that facilitated cybercrime.⁶⁶⁵ These best practices included an Antibot Code of Conduct, which encouraged ISPs to engage in “(1) end-user education to prevent bot infections; (2) detection of bots; (3) notification of potential bot infections; (4) remediation of bots; and (5) collaboration and sharing of information.” ISPs in the Netherlands are loosely organised. ISPconnect and the Dutch Hosting Provider Association are associations of ISPs, but only a minority of ISPs are a member of either of these. Furthermore several ISPs are a member of Nederland ICT. Although ISPs may discuss best practices and try to take preventive action on a voluntary basis, there are as yet no binding standards or rules. In The Netherlands, there are numerous initiatives where organisations such as ECP.nl, corporations, government and NGOs cooperate to improve (the use of) IT in the Netherlands. Several projects involve education to improve end user security awareness.

At present ISPs appear to do take significant action to prevent and combat cybercrime, both individually and collectively. These actions, however, are still only taken on voluntary basis. ISP best practices are a promising development which – if sufficient room is provided by privacy regulation, see sections 7.4 and 8.2 – may eventually help in combating cybercrime.

662 Cf. OECD 2012a: 50, recognising the need for governments to foster the development of standards.

663 Mehra 2010: 684-685, citing a brief from the USIIA in a 2006 court case. See also Rowe a.o. 2011, noting the role of the FCC, and describing international developments.

664 For example in 2005 the Federal Trade Commission (FTC) encouraged ISPs to action: http://www.theregister.co.uk/2005/05/24/operation_spam_zombie/.

665 <http://www.fcc.gov/document/csrc-adopts-recs-minimize-three-major-cyber-threats>, and <http://www.fcc.gov/document/fact-sheet-csrc-recommendations>, see also <http://www.infoworld.com/article/2619627/network-security/u-s--isps-commit-to-new-cyber-security-measures.html>. In July 2014 the FCC requested comments on implementation of these best practices: <http://www.fcc.gov/document/pshsb-seeks-comment-csrc-iii-cybersecurity-best-practices>

Software vendors. In the U.S.A. the Software and Information Industry Association (SIIA) organises software vendors.⁶⁶⁶ In the Netherlands, the most important industry association is Nederland ICT.⁶⁶⁷ This organisation regularly publishes revised model general terms and conditions, which are used by many Dutch IT companies. These terms and conditions are perceived as relatively favourable to IT companies and less so to their clients.⁶⁶⁸ These conditions aim at taking the most recent technological developments into account as well as the latest legal developments regarding IT. Although the industry recognises numerous competing standards and methodologies for software development, an IT company is only obliged to follow these if the contract contains an obligation to this end. At present there are no indications that contracts regularly contain express obligations to observe specific standards so as to ensure software security. The standards that are referred to are mostly internationally recognised standards. There is not an abundance of public documentation of software vendors on standards and other practices that are applied.⁶⁶⁹ The lack of discussion hinders learning of earlier mistakes and thereby limits the possibility of developing practical, effective standards. Nonetheless there is reason to assume that most major companies do take security seriously and do take action. However, such a positive attitude is not obligatory and may not be universally adopted. Furthermore, the actions taken at present still do not appear sufficient to prevent the occurrence of many vulnerabilities in widely used mass market software.

A large number of software development standards have been developed, many of them by prominent standard-setting organisations such as ISO,⁶⁷⁰ IEEE⁶⁷¹ and IEC.⁶⁷² These standards are not always publicly (freely) available. They have been adopted at various rates within the industry. Regardless of the merits of these standards, and the contribution they may have had to increase the level of security compared to what it was before, the fact remains that these standards at present have not managed to prevent all vulnerabilities even for the companies that adopted them.⁶⁷³ The International Telecommunication Union⁶⁷⁴

666 <http://www.siia.net/>

667 See www.nederlandict.nl, the successor of ICT Office and earlier the FENIT.

668 As regards the earlier versions see Kruijer 2000, De Graaf 2006.

669 This may be caused partly for reasons of protection of business secrets, partly also because such publication might actually help cybercriminals to find oversights.

670 See in particular ISO/IEC 27001 which specifies an Information Security Management System to manage information security risks, and ISO/IEC 27034 regarding secure software development, also ISO/IEC 27014 and ISO/IEC 27018.

671 Institute of Electrical and Electronics Engineers (an American professional association).

672 International Electrotechnical Commission, see <http://www.iec.ch>.

673 As evidenced by most major companies still being plagued by vulnerabilities: either these standards are not accepted by any major company, or some of these companies have adopted these standards without completely eradicating vulnerabilities. See further s. 4.4.3.

674 A UN agency, see <http://www.itu.int/en/about>.

has been involved in combating cybercrime.⁶⁷⁵ One particular initiative (still in progress) is the development and investigation of ICT standards to improve security.⁶⁷⁶ One effort has been the categorisation of approved standards in a database.⁶⁷⁷ The mere existence of such a database already indicates the practical failure of current standardisation in this area, as the existence of multiple standards means in practice that there is not one widely-used standard. Nonetheless there may be some feasible, effective standards available that simply have not found universal adherence. This would be a subject for further, IT-specific research.

There are no clear indications that professional or business organisations may play a large role to improve the quality of software. Although the reputation of software vendors as a group would arguably benefit from higher quality software, the main obstacles in reaching that goal appear at present to be not merely the lack of standards or best practices, but also the lack of compliance with such standards in practice (possibly caused partly by a lack of security awareness and strong economic disincentives (s. 4.4.3)). Business organisations lack the resources to counter these influences; in particular, they cannot enforce group compliance, even if that would be in the interest of the group. This is compounded by the fact that there is no mandatory membership in such organisations: software may be developed and published by anyone. Although many software vendors may actively work towards providing secure software, there is no legal sanction if a specific vendor neglects to do so, thereby gaining an advantage of other business who do spend time and money to prevent vulnerabilities.

Businesses. Businesses (in particular in specialised industries, such as health care or finance) may exchange the experiences they have with data breaches and DDoS attacks,⁶⁷⁸ possibly with the help of external IT service providers. The U.S. Federal Financial Institutions Examination Council (FFIEC) has, for example, issued a statement⁶⁷⁹ that their members⁶⁸⁰ expect financial institutions to take a number of specific steps to mitigate the risk of DDoS attacks. The statement does not appear to contain strict legal obligations, but it

675 See also the UN resolution 55/63 of 4 December 2000: Combating the criminal misuse of information technologies.

676 <http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx>,
<http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/default.aspx>.

677 http://www.itu.int/ITU-T/security/main_table.aspx

678 FFIEC Joint Statement Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources (April 2014), available at <https://www.ffiec.gov/press/pro40214.htm> and <https://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf> See further <https://www.ffiec.gov/cybersecurity.htm>

679 The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

680 See also the earlier Februari 2013 alert of the NCUA,

may have legal repercussions if it is not followed. As there is a large variety of sectors and businesses which adopted self-regulatory instruments, an exhaustive overview cannot be provided. It would also not contribute to the question which duties actually exist.

*Internet architecture organisations.*⁶⁸¹ One particular form of soft law is the institutional organisation of the Internet. The Internet is constituted by a set of protocols and standards that govern the communication between the servers and clients that make up the Internet,⁶⁸² as well as the applications that use the Internet and are often identified with it.⁶⁸³ Another option, apart from the improvement of software security by avoiding bugs, might be to modify the Internet communication protocols in order to make measures against cybercrime easier (for example, to facilitate the tracing of botnet commands).⁶⁸⁴ However, this would be a complicated technical matter, perhaps difficult to realise, and it might lead to less efficient (hence slower) Internet communication. It may also run into political and legal difficulties, including conflicts with principles like net neutrality and privacy. As communication protocols are not within the scope of the present research, we will not discuss this issue further.

6.6.4. *Specific intermediaries*

Another manner in which cybercrime can be regulated is through specific intermediaries, other than ISPs, which are part of the various business chains involved in software and Internet technology. A prominent example is the app store. App stores function as gate keepers for a part of the market.⁶⁸⁵ These stores could, in principle, apply particular requirements as to the quality of the software offered through the store. This control is, however, not absolute. An app store owner is not in the position to exhaustively check for the absence of vulnerabilities.⁶⁸⁶ Nonetheless, some improvement may be obtainable through specific demands. Examples are:⁶⁸⁷

681 Cf. Brenner & Clarke 2005: 28, 33. A description of organizations responsible for Internet architecture is generally to be found under the heading of Internet governance, see for example Bygrave & Bing 2009 and Schermer & Lodder 2014.

682 Such as the IP and TCP protocols.

683 Such as the File Transfer Protocol (FTP), e-mail protocols such as POP3.

684 See the critical discussion (with references) in Barnes 2004: 286-287, see also OECD 2008: 53 that states "Technical measures such as filtering, DNSSEC, sinkholing and many others could be examined to understand how they would help fight malware." Such techniques might be facilitated by changes in Internet protocols.

685 They are not absolute gatekeepers, as it remains possible to install software outside such stores.

686 In particular as many legitimate applications may exhibit network behaviour superficially similar to that of malware, such as interaction with a centralised server, sending IP requests to third party web-sites.

687 Partly inspired by Warner & Sloan 2012.

- requiring the notification or publication of which security standards or practices are adhered to,
- requiring the adherence to these security standards to be subjected to external auditing,
- in the absence of any auditing and/or standards or practices; the requirement to explain how security is safeguarded,
- the grading of security of software on the basis of the information provided,
- imposing a 'security surcharge' for software for which the developer did not provide sufficient material on security quality.

There may be reasons for a specific app store to abstain from some or all of these possible demands, for example because of the competition between app stores. Nonetheless, there are measures which could be taken. However, these intermediaries cannot be held liable for insecure software offered in their store, given the conditions under which such stores operate. Imposing mandatory liability appears to go too far: this would lead to a high degree of intervention in which software is available, which the majority of computer users apparently finds undesirable.⁶⁸⁸ This measure could bring about a situation in which third parties can decide what software an individual user can install on his computer.

6.6.5. *Arbitration*

As a final note, a brief remark about alternative dispute resolution, in particular arbitration, is provided. Arbitration in itself does nothing to improve compliance with duties of care and diligence, given the restrictions detailed in par. 5. Only in specific, relatively close-knit sectors with few businesses may the existence of a customary single arbitration court provide additional incentives for businesses to comply. In the construction industry or in finance there are indications that arbitrators who originate from the industry are stricter because they know precisely what measures can be taken and can reasonably be expected. Companies in such a sector might fear reputational damage amongst their peers, which might stimulate voluntary compliance. A provisional analysis of the software industry suggests that this sector is too diverse for such mechanisms to operate.

Furthermore, it does not at present appear to be feasible to stimulating arbitration. Attempts at including arbitration clauses in software agreements are currently looked at with suspicion, as it is rather feared that this would lead to outcomes even more favourable for the software industry. Although arbitration might offer lower costs for the plaintiff (if the rule would be that the software vendor would have to bear the costs of arbitration in most cases) and overcome possible problems with international litigation and enforcement,⁶⁸⁹ this currently is not a feasible prospect.

⁶⁸⁸ Cf. s. 8.3 on stricter regulation of available software.

⁶⁸⁹ An example of a successful arbitration arrangement is the ICANN arbitration for domain name disputes.

6.7. Conclusion

There is relatively little enforcement of the duties of care and diligence that were found. The primary reason is that the costs of a procedure outweigh the possible award of damages. Furthermore, there are difficulties with the proof of causality relating to contributory causes. Collective action may be more successful in some cases.

Furthermore, the effect of notification duties on insurance currently stands out among the alternative compliance mechanisms.

7. International norms for prevention of cybercrime

7.1. Introduction

Cybercrime has received much international attention.⁶⁹⁰ There have been many reports,⁶⁹¹ investigations and discussions. There are, however, few specific norms.

7.2. Private law

There are relatively few supranational or international private law norms that impose duties of care and diligence. For the present research the only relevant norm is arts. 12-15 E-commerce Directive 2000/31/EC, which provides ISPs with an exemption of liability for the information which is transmitted or hosted, on the condition that (to paraphrase) the ISP remained passive with respect to the information.⁶⁹² Once the ISP is informed of the unlawful nature of the content, the ISP no longer qualifies for this exemption and will usually need to remove the information or disallow access (Notice and Take Down).

7.3. Criminal law

There is considerable international activity in criminal law which targets cybercrime. Most of these measures, however, are regionally oriented or cover other cybercrimes than those that are the subject of this report.⁶⁹³ We will focus only on those initiatives which bear direct relevance to the current research.

One of the major successes in the international field is the Budapest Convention on Cybercrime of 23 November 2001.⁶⁹⁴ The convention obliges member states to establish specific cybercrimes as criminal offences. These include, as far as relevant here, obtaining illegal access to a computer (art. 2), illegal interception of data (art. 3), data interference (art. 4, which includes damaging or deleting data), serious hindering of the functioning of a system (art. 5, which may involve transmitting data), and the making available devices, including computer programs, that aid in the aforementioned offences (art. 6). Article 11 stipulates that also aiding and abetting these offences need to be criminalised, but since this is limited to intentional aiding and abetting 'with intent that such offence be com-

690 See also materials and references on <http://www.cybercrimelaw.net/Cybercrimelaw.html>

691 For example the oft-referenced OECD 2008 report, Schjølberg & Hubbard 2005, ITU 2011, studies under the United Nations Office for Drugs and Crime (UNODC) such as UNODC 2013, <http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf>, and cf. <http://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html> and see its legislation database at <http://www.unodc.org/cld/index-sherloc.jsp>

692 See the more detailed discussion in s. 5.2.2.

693 See the overview in UNODC 2013: 63-76.

694 <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. See relevant reports on http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp. As regards the implementation of the convention see http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study2-d-version8%20_28%20august%2008.pdf

mitted', this will not apply to ISPs or software vendors who do not fulfil duties of care and diligence (unless they knowingly build in bugs in software in order to facilitate cybercrimes).

Furthermore, the convention obliges member states to have sufficient investigation powers in place to enable cyber-investigations,, such as the obligation to preserve and disclose traffic data (art. 17), search and seizure of stored computer data (art. 19), real-time collection of computer data (art. 20), and interception of content data (art. 21). Finally, to facilitate mutual assistance among party states, the convention contains many provisions on mutual cooperation and assistance (art. 23-34).

The EU has adopted the Directive 2013/40/EU of 12 August 2013 on attacks against information systems. It establishes minimum rules regarding the criminal sanctions for attacks on information systems. This replaces EU Framework Decision 2005/222/JHA on attacks against information systems. Art. 8(1) Directive 2013/40/EU obliges Member States to ensure that aiding and abetting the offences of art. 3 through 7⁶⁹⁵ is also a criminal offence. However, the offences require criminal intent;⁶⁹⁶ hence it is to be assumed that only aiding and abetting with criminal intent is to be made punishable.

These initiatives are only tangentially relevant to the present research, as they mostly aim to clarify that the criminal activities themselves are to be punishable without saying much about obligations to take preventive action resting on other parties.

7.4. ISPs, privacy rights and Internet principles

Combating cybercrime is further complicated as certain precautions and preventive measures may conflict with fundamental rights. The necessity to balance fundamental rights with crime prevention is recognised at both ends of the regulatory debate.⁶⁹⁷

The principal conflict involves the possibilities of ISPs to monitor network traffic.⁶⁹⁸ Although there are various technically feasible measures to detect suspicious traffic and to find and disable botnet clients, the actual application of such measures may violate fundamental rights or principles. As already pointed out (s. 5.2.2), ISPs are generally expected to remain neutral as to the information transmitted and stored. This role is hard to reconcile with a more active approach to monitor and filter for undesirable content. Four specific conflicts may be identified.

(1) An active ISP may no longer qualify for the exemption of liability, as it applies only to ISPs that remain passive. As discussed above, most legal systems only exempt passive

695 Involving illegal access to information systems, illegal system interference (among which DDoS attacks), illegal data interference, illegal interception, and misuse tools for committing said offences.

696 See cons. 17 Directive 2013/40/EU.

697 For example cons. 28 Directive 2009/136/EC recognises that net neutrality must not prejudice the requirements of security of the network.

698 See also Martin & Andrade 2012, and compare Rowe a.o. 2011, also Pannetrat 2011.

ISPs from liability, although the U.S. is a major exception by allowing ISPs to more actively filter for some kinds of illegal content without thereby necessarily losing their exemption.

(2) ISPs may be forbidden by public law to discriminate between various forms of content. This is a side-effect of the discussion on the principle of *net neutrality*. This principle basically states that ISPs have to treat all traffic equally and may not block or otherwise hinder the transmission of certain content.⁶⁹⁹ This principle is currently being debated in various jurisdictions,⁷⁰⁰ while it has been established in statutory law in a few jurisdictions, including the Netherlands (s. 5.2.4) and Brazil.⁷⁰¹ The Dutch implementation of this principle does allow an exception in case of security.⁷⁰² However, it is not always easy to determine with sufficient certainty that specific content or traffic supports cybercrime. For example, in case of a DDoS attack it would make sense to delay all requests sent to the website server that is under attack. However, some of those requests are bound to be bona fide requests made by innocent users.

An ISP which is too active in delaying communication from suspected malware may easily be accused of illegally discriminating against a legitimate application,⁷⁰³ particularly if the malware is connected with or integrated with a legitimate application.⁷⁰⁴ The risk that the ISP may incur heavy fines⁷⁰⁵ if found to be in violation of net neutrality strongly discourages a more active approach.

(3) An ISP may wish to block a computer that has been infected with malware. However, this is only possible by disallowing the owner of the computer access to the Internet. Various jurisdictions find that such measures are disproportional and require an ISP to at least provide advance warning.⁷⁰⁶ This limits the possibility of quick responses to, for example, an ongoing DDoS attack. Even if advance warning is provided, ISPs appear not to be very active in blocking suspected botnet clients. It is not entirely clear whether this is because they are unsure whether a customer's computer is actually hosting a botnet clients, because ISPs do not actually try to find botnet clients, or because they are unwilling

699 Field 2010, Wong 2011.

700 See on the currently developing FCC stance <http://www.fcc.gov/openinternet>. The earlier 'Open Internet Order' was partly upheld and partly vacated by the U.S. Court of Appeals, District of Columbia Circuit, 14 January 2014, (Verizon v FCC), no. 11-1355, see [http://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/\\$file/11-1355-1474943.pdf](http://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf). On earlier attempts see Wong 2011.

701 See art. 3(IV) and 9 Marco Civil.

702 Note that in Brazil art. 9 Marco Civil does not appear to recognize such an exception.

703 Cf. Murtagh 2009, arguing that blocking sites for copyright infringement may deprive users also of lawful content and should therefore not be allowed by the FCC.

704 Such as malware in the form of a browser extension.

705 In The Netherlands two telecommunication companies providing Internet access were fined EUR 200,000 and 250,000 in January 2015: <https://www.acm.nl/nl/publicaties/publicatie/13762/Boetes-KPN-en-Vodafone-voor-overtreden-regels-netneutraliteit/>.

706 For The Netherlands see s. 5.2.4.

to actually combat cybercrime by cutting off consumers from the Internet.⁷⁰⁷

Admittedly, this measure may not directly lead to the desired result of users cleaning their computers. A user may simply lack the expertise to clean the computer himself and may not have sufficient funds to hire an expert to do it for him. The malware may be hard to find and remove. Hence an Internet ban might turn out to be semi-permanent for a large number of users. Given the importance of Internet access in society, which tends to be viewed as close to a fundamental right, such an effect is generally considered undesirable.⁷⁰⁸

(4) ISPs might actively try to determine which of their customers have been infected with malware. An ISP may monitor traffic, in particular when spam is sent out or a DDoS attack is in progress. This would presumably lead to a list of suspected customers or IP addresses, which may be verified after additional activity has been observed. However, such monitoring may, dependent on the applicable rules, be viewed as a violation of privacy.⁷⁰⁹ Monitoring in this way requires storage of personal data (including IP addresses and traffic patterns), an examination of actual content (in order to detect communication with the bot herder),⁷¹⁰ or similar activities. All of this is highly controversial. Furthermore, criminals may complicate such activities by using proxies⁷¹¹ or other techniques to hide the actual IP address of the computer infected by the malware or botnet client.

The conclusion is that a more active ISP may quickly run afoul of fundamental rights as they are presently conceived and explicated in more detailed rules. This is not to say that fundamental rights are incompatible with the prevention of cybercrime. It does, however, mean that in order to motivate ISPs to become more active, it is necessary to provide more clarity as to which actions by ISPs are allowed and which are not. It is necessary to rethink and revise current rules in order to find a proper balance between privacy (and related rights) and cybercrime prevention.⁷¹²

707 Assumedly most ISPs do have contractual provisions that allow them to remove Internet access in the case of illegal activity from their computer.

708 See La Rue 2011, and cons. 29 of Directive 2013/40/EU, also the decision of the French Constitutional court of 10 June 2009, no 2009-580, English translation available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf.

709 Martin & Andrade 2012, Morrison 2011 regarding mail inspection.

710 Called 'deep packet inspection', which is controversial and may be illegal in some jurisdictions.

711 Albeit an ISP might during a DDoS attack cut off requests sent through proxies, this could also hinder regular traffic and might again be considered to violate the principle of net neutrality.

712 Cf. the conclusion of Martin & Andrade 2012.

7.5. Conclusion

The international norms that can be found at present are of limited value to prevent cybercrime through the imposition of duties of care and diligence on victims or third parties. International norms that aim at legal harmonisation are either directed at criminals and accomplices only (such as the Cybercrime Convention), or aim at guaranteeing Internet freedom but thereby stand in the way of preventive duties against cybercrime. In particular the application of fundamental rights of privacy and receiving information and the principle of net neutrality in an extensive manner is hard to reconcile with a more active role of ISPs, as ISPs would have to monitor, filter, and block content associated with cybercrime. Although these rights and principles do allow exceptions for the prevention of abuses and criminal activities, these exceptions are not yet sufficiently elaborated to give ISPs the required guidance as to what is to be expected from them.

The norms that exist as regards software quality have not obtained sufficient general recognition and adherence to operate as a general standard.

8. Improving compliance

8.1. Introduction

The picture described thus far contains only limited legal duties of care and diligence to aid in the prevention of cybercrime. Insofar as these duties exist, they are, furthermore, hard to enforce. Following on the previous two chapters, we will in this chapter investigate some alternative means to stimulate compliance with any duties of care and diligence, whether these are legally recognised duties or socially desirable duties to do more to combat cybercrime. We will discuss several suggestions found in the literature,⁷¹³ as well as suggestions that are inspired by other approaches discussed here.

It should be noted that these suggestions generally attempt to avoid laying further burdens on responsible companies that already follow and promote secure practices. The aim is rather to provide such companies with a level playing field, by forcing less responsible companies to spend the same amount of effort. Furthermore, the suggestions aim at providing companies who for example desire to contract for secure software or services with additional tools to actually allow them to do so.

8.2. ISPs

As the analysis of the position of ISPs makes clear,⁷¹⁴ although ISPs are strongly incentivised to combat cybercrime⁷¹⁵ they may not fully act on those incentives because they are confronted with conflicting duties of care and diligence. On the one hand they are presumed to be responsible for neutral, private, unhindered Internet communication on behalf of Internet users, but on the other hand they are supposed to be responsible for active monitoring of Internet traffic in order to prevent cybercrime on the Internet, again on behalf of Internet users. Current legislation strongly stresses the former duty, while many policy makers and legal scholars argue for the latter duty. The conflicting duties, and legal limitations to act, can schematically be presented as follows.

⁷¹³ See also Moore 2010, who focuses more on disclosure.

⁷¹⁴ See particularly s. 7.4.

⁷¹⁵ OECD 2009: 89-102.

If we wish to improve matters, the first step would be to decide and acknowledge that a strictly neutral Internet with open communication is not the only relevant value. If it would be decided that an open Internet is more important than combating cybercrime, we can uphold the current legislative status quo,⁷¹⁶ but in that case one should acknowledge that cybercrime is the price we pay for our principles.

If it is decided that conflicting duties have to be further balanced, the existing rules should be revised to openly recognise the conflict,⁷¹⁷ thereby allowing sufficient room for ISPs to determine an appropriate policy to balance the demands of neutrality (including privacy) and security. Currently the rules regarding net neutrality and privacy are highly restrictive. The phrasing of the security exceptions to these principles suggests that ISPs run a high risk of violating neutrality and privacy rules if their actions are found not to fulfil the precise criteria for an exception on behalf of security.⁷¹⁸

Similarly, the immunities for civil liability of ISPs provide strong incentives to remain passive.⁷¹⁹ They provide a chilling effect⁷²⁰ against more active monitoring, as evidenced by the U.S. experience. Given the fact that ISPs have conflicting duties, it is unavoidable to allow them some discretionary room to decide how to balance these duties.⁷²¹ Good faith efforts to achieve such a balance should be encouraged instead of punished.

Hence ISP should not directly lose their immunity for liability merely because they have taken action to filter undesirable content. An exception can be made for negligence bordering on intentionally cooperating with criminals. It is possible that in the future, if more experience has been gained, the immunities may be reconsidered in case ISPs have failed to observe even minimal standards of security.

Furthermore, rules on net neutrality and privacy should allow more room for a discretionary balancing of the conflicting interests or principles. The consequence may be that different ISPs have different policies: while some may prioritise privacy, others may stress security. This need not be undesirable, as long as users have sufficient options and do not face unduly high financial burdens to obtain connectivity to the service of their choice. Such diversity may indeed provide room for experiences as to which practices work and which balance is favoured by the markets.

Diversity in policies may also provide added incentives for ISPs to take into account the interests of security. Although bona fide ISPs already have significant incentives to pre-

⁷¹⁶ As for example argued by Harper 2005.

⁷¹⁷ Cf. ENISA 2011: 4, 126-127.

⁷¹⁸ Cf. Brenner & Clarke 2005: 39, arguing for allowing filtering and blocking.

⁷¹⁹ See also the discussion in Ziniti 2008.

⁷²⁰ Cf. Prins & Schellekens 2004 and 2005.

⁷²¹ An interesting and somewhat similar alternative is the notion of allowing ISPs a 'graduated response', as detailed by Hua 2014.

vent and combat malware as it interferes with regular Internet traffic,⁷²² these incentives may still be insufficient to stimulate further experiments with the development of best practices and standards. Additional incentives⁷²³ could be found, for example, if ISP customers could contract for security and would have an actual remedy in case of a breach of warranties regarding security.⁷²⁴ Various legal instruments are possible, such as mandatory implied warranties, a prohibition of full exclusion of economic loss, or a mandatory minimum amount of liquidated damages. The selection of ISPs with proper attention to security might even become part of the assessment of a business' security measures, providing further incentives for ISPs to take account of security.⁷²⁵ A non-legal measure would be a mandatory government standard for procurement of ISP services, which would demand heightened security services: this would stimulate a market for upmarket security ISP service.

As ISPs currently already appear to discuss and exchange best practices as regards security efforts, there are sufficient indications that a thriving practice of care and diligence towards security may develop. Additional softer measures might be notification and publication duties for security breaches, incidence of malware, amount of originating of DDoS attacks, and the efforts taken to prevent and detect malware.

For specific measures that have already proven to be feasible and effective, explicit rules in administrative law may be appropriate.⁷²⁶ Examples that are currently still controversial but might be effective are take down orders for websites found to intentionally distribute malware,⁷²⁷ injunctions to avoid a private party registering and operating a certain domain name,⁷²⁸ and measures against 'rogue ISPs'.⁷²⁹ Whether such measures are to be adopted or, on the contrary, are to be avoided because of the principles of net neutrality or an open Internet, is the domain of politics. We only point out the possibility of such measures.

Appropriate standards of care should be developed and enforced by the involved parties themselves.⁷³⁰ Government regulation and enforcement is to be reserved for extreme cases only.

722 Cf. Mann & Belzley 2005: 304, OECD 2009: 89-110.

723 ENISA 2011: 128 remarks on the need for additional incentives.

724 Cf. Brenner 2004a, arguing for secure portals, and Gijrath 2012.

725 Brenner & Clarke 2005: 38 and 46, suggesting also licensing of ISPs.

726 Sherling (2014: 596 and 606) argues for FCC imposed standards, or alternatively for a duty of disclosure by the ISP of the security practices followed. On p. 605 he proposes also certification.

727 Cf. on an Australian case <http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/> and <http://www.zdnet.com/article/website-blocking-is-not-internet-filtering-australian-government/>.

728 Cf. on an attempt to forbid the use of 'piratebay.se': <http://www.thelocal.se/20150210/swedish-court>.

729 ISPs that intentionally neglect to take even basic security measures, see OECD 2009: 102.

730 This is in line with the suggestion of fostering partnerships with ISPs (OECD 2012a: 45, OECD 2012b).

8.3. Software vendors

As discussed above (s. 4.4.3), software vendors as a group currently do not have sufficient incentives to spend much effort on improving software security in order to avoid vulnerabilities. The legal framework presently does not enforce duties of care and diligence for software security. Liability only exists for defects that were known but not communicated, or defects that became known at a later time and were not patched with sufficient speed.⁷³¹ The problem here appears to be not only a lack of a legal duty of care and diligence, but, more importantly, that there are strong disincentives to taking the extra effort for secure software. There is a premium on being first to market with new functionality, while users do not discriminate between secure and insecure software when making the decision to buy a particular software package. Although the legal framework allows software vendors large discretion as to how to develop software, this discretion is not universally used to adopt good security practices. Thereby software vendors who do take efforts for secure software are disadvantaged compared to vendors who disregard security, as the latter group saves time and money. Schematically this may be described as follows.

The problem with insecure software is exacerbated by the lack of a community: software vendors (and developers) as a group do not as a matter of course discuss amongst each other good development practices with a view to improve security. Even though specific large software companies and/or companies within their network may have developed a culture of security with open discussions and proper standards, this is not shared with other companies, let alone the software sector as a whole.

In other sectors the answer would be stricter regulation of the sector. In the case of software, this solution is not to be recommended as this would amount to the institutionalisation of strict regulation of the software industry by requiring software engineers and programmers to follow formalised education programs and take entry exams, similar to

⁷³¹ An exception appears to be Brazilian law.

the arrangements in regulated professions like doctors and lawyers or advocates. Although such a measure would probably raise security awareness in the profession, it does not appear to be feasible. The resulting costs would be disproportionate for most software companies. Furthermore, this would effectively end the tradition of ‘garage’ startups formed by enterprising individuals without formal diplomas.

A slightly different approach would be to tackle the other end of the distribution chain: imposing entry barriers for the publication or distribution of software. However, this again appears to be infeasible as consumers prefer the freedom to install the software they desire,⁷³² regardless of where they found it.

Nonetheless, this approach allows for a ‘softer’ incentive. Governments could provide market incentives for better security by requiring government organisations to demand higher security and quality standards for the software being procured, including what is called ‘security by design’. The ‘carrot’ of government contracts might induce at least part of the market to improve standards and practices.⁷³³ However, this is still not a complete solution as there are apparently currently no clear, generally accepted standards that guarantee the absence of vulnerabilities.⁷³⁴ Software vendors could simply go through the motions by advertising very general standards and practices without actually achieving superior security. Care should be taken to adopt standards that provide actual improvements to security. Incidentally, this approach of procurement standards could and should be extended also to other IT services.

Because of the absence of clear effective standards that are universally recognised it is also not an option to impose strict regulation of software development.⁷³⁵ In other words: there is as of yet no practice of care and diligence. Hence the solution would be to provide incentives to foster such a practice.⁷³⁶

A simple, albeit controversial, solution would be to adopt a form of product liability for software. This has already been advocated by many scholars (s. 5.3.2.3). The law would then have to recognise a liability for unknown (but knowable through best effort or due care) defects.⁷³⁷ This would have to be coupled with a restriction to the extent to which liability may be excluded by contract, and with provisions that allow the recovery of pure economic

⁷³² See also Chandler 2004: 243 and 254-255, referencing Zittrain, for the undesirability of limiting users’ control of which software to install.

⁷³³ Cf. Almond 2009, arguing that business purchasers should ask for security, driving up the market for everyone. Also Gijrath 2012, OECD 2012a: 50.

⁷³⁴ This is deduced from the fact that such a standard, if adopted by a company, would lead to vulnerability-free software, which however at present is inexistent and is even said to be impossible.

⁷³⁵ Otto 2009: 342.

⁷³⁶ Otto 2009 argues therefore for (broad) standard based regulation instead of detailed standards.

⁷³⁷ Pinkney 2002: 72.

loss or of a fixed amount, possibly allowing or mandating punitive damages in aggravated circumstances. Even if individual customers would still have insufficient incentives to instigate an action, the threat of collective action (such as class actions) would incentivise software developers to strive towards higher security standards.

However, such an approach is not unproblematic. It would strongly disincentivise the provision of free software.⁷³⁸ By raising the general costs of making and selling software it would impose a high barrier of entrance to the software market. This would arguably stifle innovation in software.⁷³⁹ One should bear in mind that, in contrast with the automobile industry (to which the software industry is often compared), software is a low-cost, low-priced product with small development investments and with many competitors, instead of the oligopoly that automobile manufacturers, who were perfectly capable of taking extensive measures to improve product safety, form. For cases of gross negligence towards security there may already be a remedy in most jurisdictions.

A more practical alternative is to focus only on the main source of malware infections, to wit widely used mass-market software. Criminals focus on widely used software as this provides the highest returns on infection. Even if only mass-market software is made more secure, this could provide a significant reduction in the incidence rate of cybercrime. Furthermore, such software is commonly produced by large companies who arguably are in a position both financially and technologically to take a significant effort to improve security. Product liability for software might therefore be limited to mass-market software that has reached a certain level of market penetration. However, this still seems to be a measure of last resort, as the consequences towards liability appear possibly disproportionate to the effect desired. Furthermore, it should be noted that this does not address widely used free software.⁷⁴⁰

For free software (including Open Source software) a possibility could be assuming an obligation of a business to ensure a minimum level of security of the software used. Such an obligation may actually be assumed also in the case of commercial software. For commercial software the vendor might have a duty to check for and avoid vulnerabilities, and businesses often have a support contract with the vendor that supposedly would provide the business among others with a right to receiving patches for any vulnerabilities discovered. However, a support contract is not mandatory, and patches may be received also without a support contract. In case free software is used, a support contract is less

⁷³⁸ Unless the rules only apply to software provided for monetary consideration. However, this begs the question as to how to classify apps provided for free, but consideration is found in extensive usage of the customer's private data by the vendor.

⁷³⁹ Cf. Weber 2012: 479-480, Pinkney 2002: 72.

⁷⁴⁰ Such as the Apache webserver, or the Single Sign On (SSO) protocol software which was affected by the HeartBleed vulnerability.

common, while there is no right to receive patches or a duty on the developers to avoid and check for vulnerabilities. For such software the obligation to ensure a minimum level of security might entail that the business should hire an IT service provider who will check the software for vulnerabilities and provide patches.⁷⁴¹ Thereby there would be an incentive for such activities for free software too. This would allow for spreading the costs of security efforts over the businesses that benefit from it.⁷⁴²

An alternative is to create market incentives through information duties. These can comprise the labelling of security measures⁷⁴³ and a duty of disclosure or notification of vulnerabilities (possibly not publicly but only to a government agency). Like in the food industry, mandatory labelling may encourage consumers to become aware of the security aspect of software.⁷⁴⁴ Even if not all consumers will be interested in this aspect, it might again influence at least part of the market, which might turn the tide. It should, however, be admitted that presently consumers apparently do not even care about highly publicised vulnerabilities in software. Furthermore there are companies that claim that publicly making measures available will only aid criminals and not contribute to a higher degree of security.⁷⁴⁵ It should be noted that information may be provided in various degrees, and not all suggestions require publication of all measures to the general public.

A more important measure would be to couple labelling rules and notification rules with mandatory 'lemon laws' which allow customers to return the software in case of deliberate misinformation,⁷⁴⁶ or in case certain kinds of vulnerabilities are found (in particular more egregious vulnerabilities that would have been easy to avoid). This would provide an easy remedy for customers which, in turn, might provide more incentives for software vendors to prevent such vulnerabilities. However, this again may be a disproportionate measure considered in relation to the aim of avoiding vulnerabilities.

Furthermore, mandatory labelling could encourage public discussion on appropriate security standards. It could lead to private organisations providing rankings of standards or practices. As noted above, currently there appears to be insufficient communication on an industry-wide basis to allow the development of generally adopted and implemented standards. Alternatively, the establishment of private foundations or associations which aim

⁷⁴¹ Such services do exist for open source software, see for example Red Hat, Inc.

⁷⁴² Possibly the businesses that hire such a provider would receive patches or warning earlier than others, thereby having an incentive to hire such services. Open source software generally (with some exceptions) requires improvements to be made available to the general public as well.

⁷⁴³ Brenner & Clarke 2005: 44.

⁷⁴⁴ Cf. Warner & Sloan 2012.

⁷⁴⁵ This is in essence the debate between proponents and detractors of the approach of open source software. We only point out the standpoints on either side; it requires an IT-specific research to determine which side is correct.

⁷⁴⁶ Cf. Barnes 2004.

to increase software security may provide added incentives, in particular if they can and will instigate actions against software vendors who structurally prove negligent.⁷⁴⁷

Also, private initiatives such as bounty programs might be stimulated. Funding could be obtained partly through fines imposed on software vendors whose software has been found to be deficient, in particular if the vulnerabilities can be attributed to gross negligence or if the company cannot show that it structurally takes preventive measures. Similarly, funded white hat hacking⁷⁴⁸ in order to detect vulnerabilities in widely used mass-market software might have beneficial effects.

Another possible measure is to adopt the approach used for aviation safety.⁷⁴⁹ Pilots and other aviation professionals may in several jurisdictions report incidents without thereby incurring liability, with the aim of encouraging pilots to learn from each other's mistakes. Furthermore, in the U.S.A. the National Transportation Safety Board, equipped with wide investigative powers, investigates accidents, performs studies to learn from these accidents, and publicises reports to disseminate this knowledge.⁷⁵⁰ This facilitates an inter-business learning that would otherwise not occur, and promotes a general culture or practice of aviation safety.⁷⁵¹ Notification duties may support such a 'National Cybersecurity Board' by providing additional information on cybercrime incidents.⁷⁵²

Increased liability rules and/or notification rules might also give rise to beneficial practices based on the policies of software insurance for vendors.⁷⁵³

Additional measures are to subsidise, support or encourage research on and standardisation of the prevention of vulnerabilities. Although this is not a solution in itself, it might be a crucial element of a more complete strategy.

These measures might be further strengthened by public law enforcement in cases of gross negligence.

747 Possible remedies could be injunctions or orders to take specific actions, or discovery proceedings to make clear what kind of actions are actually taken to avoid vulnerabilities. Currently such information could be hard to obtain, partly due to the fact that it may be qualified as confidential and commercially sensitive.

748 Hacking not for criminal purposes but solely to inform interested parties about the vulnerability in order for it to be corrected.

749 Cf. OECD 2012a: 50, pleading for government leadership in facilitating information sharing, also ENISA 2011: 128.

750 See 49 U.S.C. § 1131a. Several other jurisdictions have similar organisations.

751 See Kooijmans, Tjong Tjin Tai & De Waard 2014, ch. 5, also on the confidentiality of information provided to the NTSB.

752 Borgesius 2011: 217, referring to Schwartz & Janger 2007.

753 Cf. s. 6.6.2 also Levy & Bell 1990: 27 and Pinkney 2002: 73.

8.4. Businesses

At present businesses appear to have already mostly sufficient incentives to take security measures against cybercrime due to their own interests and the existing legal framework. From the viewpoint of duties of care and diligence, the occurrence of security incidents does not prove that the existing duties are inadequate; incidents are an unavoidable part of life. Admittedly, there are some disincentives.⁷⁵⁴ In particular the costs for additional security may lead to a cost-benefit analysis with the outcome that a business decides to take less security measures than desirable from an outside perspective. Furthermore the lack of expertise of a business may lead to a lower security level than desirable.⁷⁵⁵

However, if the aim is to increase the level of security provided, the following might be considered.⁷⁵⁶

With respect to security breaches due to insecure software and/or later infections with ransomware, the current framework of notification duties appears to be a largely efficient and effective method due to the involvement of the insurance industry.

A soft measures that might improve security is generally raising security awareness within industry. At present there apparently are still many businesses (particularly smaller businesses) who neglect to take some of the basic security measures that are available at low cost. This may be due to a lack of expertise or lack of awareness of the problem. One step further would be to help develop or promote a simple set of best practices to be used by businesses who want to promote security.

⁷⁵⁴ Cf. OECD 2009: 129-136.

⁷⁵⁵ As Mueller 2006 points out, cybersecurity is becoming a highly specialised subject which businesses may not be able to arrange on their own.

⁷⁵⁶ Brenner & Clarke 2005: 42-43 also suggest a duty on management to follow basic security standards. The rise of notification duties and consequent cybersecurity insurance nowadays covers this aspect. On p. 44-46 they also suggest mandatory insurance, which however has the disadvantage of not allowing insurers to refuse bad risks.

An additional measure to stimulate secure practices in businesses is to institute mandatory security audits, similar to financial audits. For specific regulated sectors there may already exist rules for security as part of regular audits. This would stimulate a market for IT security services, and lead to further discussion of secure practices. If a general obligation for security audits is found to be undesirable, this could be limited to specific sectors where security breaches would be particularly undesirable, to companies above a certain size, or in other ways. If mandatory security audits are found to be infeasible, one might look at softer means to stimulate such audits (such as requiring government contractors that handle sensitive or personal data to have such audits). Incidentally, if businesses would have to hold security audits, government organisations should be under the same obligation.

The incidence of security breaches would arguably diminish if software would be more secure (s. 8.3). For free software, businesses could provide themselves with security services by contracting for such services (s. 8.3).

As a related option: businesses at present may find it difficult to contract with software vendors or IT service providers without significant limitation clauses. Thereby businesses may not always be able to effectively enforce a duty of care or diligence violated by a software vendor or IT service provider. As a regulatory measure one could require explicit information or warning about such clauses. One step further would mandatory laws prohibiting certain forms of exclusion. However, as this could have far-reaching consequences for the whole system of private law, this is not to be directly recommended.

From the perspective of the individuals who experience a loss of personal data, additional remedies may be considered, such as allowing the recovery of pure economic loss or moral damage or a minimum amount of mandatory fixed (liquidated) damages. This could be limited to specific vital sectors, as it could be argued that customers generally should be expected to bear themselves the small loss of value incurred by temporary inavailability of a service, or to take appropriate measures for alternatives. Furthermore this could be limited to cases of gross negligence only.

With respect to DDoS attacks: the customers of businesses experience loss of service. Businesses generally already try to avoid DDoS attacks as they may cause customers to take their business elsewhere (both during and after the attack). Adding further incentives seems superfluous. If the view is that customers should have effective remedies, one may again consider recovery of pure economic loss or mandatory fixed damages.⁷⁵⁷

Furthermore, a national cybersecurity board, as discussed in section 8.3 for software vendors, might also be instituted to investigate security breaches and DDoS attacks, again with the aim of providing inter-business learning of earlier incidents.

For specific sectors, in which continuity of service is of supreme importance, more

specific legislation may be considered. It is already clear from the overview in chapter 5 and 6 that relevant supervisory agencies have taken initiatives to adopt more stringent measures. The question which specific rules to adopt relates to the technical matter of how to ensure continuity of the service in the face of a DDoS attack.

8.5. Conclusion

We have provided a number of suggestions to improve compliance. These are all aimed at stimulating good practices of care and diligence, to be strengthened primarily through private enforcement and for which public enforcement is an instrument of last resort only. These suggestions have been summarized at the beginning of this report. We should, however, not forget that these measure should be combined also with traditional public law enforcement and other governance measures. Prosecution of cybercriminals provides at the very least moral support to private initiatives, while also being effective in uprooting central causes of cybercrime. Furthermore, sufficiently keeping legislation up to date for being able to handle new forms of cybercrime is also required. These topics, however, are outside the scope of this report.

9. Conclusions

Duties of care and diligence have been used as tool to examine whether actors indirectly involved in the occurrence of cybercrime may be legally required to take preventive action and whether it is possible to provide further encouragement to action. This assumes a perspective in which private parties take the lead to developing good practices, with public regulation and enforcement primarily providing support. To avoid misunderstanding it is to be stressed that this report has been specifically requested not to examine the role of criminals, private individuals, or government as such (particular in its role as prosecuting crimes). Naturally significant efforts in these areas are also required to effectively combat cybercrime. The suggestions described in this report should therefore not be read as solely putting the burden on the actors on which this report focuses.

Although there are numerous actions that ISPs, software vendors and businesses could take to prevent cybercrime, such actions are not always taken to the fullest extent possible. This is due to a combination of economic and legal disincentives for ISPs and software vendors, as well as a lack of commitment or expertise on the part of businesses. Notwithstanding significant efforts by many of these actors, there are also numerous individual actors who do not show sufficient interest and effort towards creating a secure environment. Insofar as there is some legal recognition of duties of care and diligence to act against cybercrime, actual enforcement of such duties is difficult due to limitation of damages and problems of proof. There are few hard, easily applicable and enforceable standards.

Several measures are conceivable that might encourage further action. These have been listed at the section 'Possibilities for improvement' at the beginning of this report. It should be noted that such actions will not completely prevent cybercrime, if only because one of the causal factors of cybercrime is a lack of security awareness of private users, which is hard to remedy and is outside the scope of this report.

The measures suggested comprise a variety of means with the focus on

- providing private parties sufficient discretionary room to allow them to determine best practices and standards, using the contextual knowledge at their disposal, tailored to the specific circumstances in which they are involved,
- adding (further) incentives and removing disincentives to actually take measures for further care and diligence,
- encourage public exchange of information to foster a culture of care and diligence, providing opportunities for learning from each other's experiences.

In addition private mechanisms, such as beneficial influences of insurance, and public enforcement, in case of gross negligence, may strengthen such measures.

By encouraging and to a certain extent institutionalising such duties of care and diligence against cybercrime, a culture of Corporate Digital Responsibility may be promoted.

Annex 1. Bibliography

- Alces, Peter A. (1999).** 'W(h)ither warranty: the B(l)oom of products liability theory in cases of deficient software design', *California Law Review* 1999, Volume 87, Issue 1, p. 269-304.
- Almond, C. (2009).** 'Should Vendors Be Liable for Security Flaws in Software?', *Computer Fraud and Security* 2009, Issue 4, p. 4-7.
- Amadei, X. (2001).** 'Standards of Liability for Internet Service Providers: A Comparative Study of France and the United States with a Specific Focus on Copyright, Defamation, and Illicit Content', *Cornell International Law Journal* 2001, Volume 35, Issue 1, p. 189-230.
- Baas, J.A.N. & Rest, M.H.J. van (2012).** 'Informatie- en meldplichten bij datalekken en beveiligingsinbreuken', *Privacy & Informatie* 2012, p. 260-268.
- Bar, Ch. von (2009).** *Non-Contractual Liability Arising out of Damage Caused to Another*, Principles of European Law (PEL Liab. Dam.), Oxford: Oxford University Press 2009.
- Bauer, M. & Eeten, M.J.G. van (2009).** 'Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options', *Telecommunications Policy* 2009, Volume 33, p. 706-719.
- Barnes, Douglas A. (2004).** 'Deworming the Internet', *Texas Law Review* 2004, Volume 83, Issue 1, p. 279-329.
- Beau Baez III, H. (2014).** *Tort Law in the United States*, Alphen aan de Rijn: Kluwer Law International 2014.
- Beraldo, Leonardo de F. (2004).** 'A Responsabilidade civil no Parágrafo único do Art. 927 do código civil e alguns apontamentos do direito comparado', *Novos Estudos Jurídicos* 2004, Volume 9, Issue 2, p. 317-340. Available at: <http://www6.univali.br/seer/index.php/nej/article/download/367/310>
- Berkvens, J.M.A. & Prins, J.E.J. (2014).** 'De bescherming van persoonsgegevens', in: Van der Hof, Lodder & Zwenne 2014, p. 179-212.
- Bernstein, Herbert (1998).** 'Civil Liability for Pure Economic Loss Under American Tort Law', *The American Journal of Comparative Law* 1998, Volume 46, p. 111-132.
- Bernstein, Hebert L. (2002).** 'Contracts' in: David S. Clark & T. Ansay, Introduction to the law of the United States, The Hague – London – New York: Kluwer Law International 2002, p. 159-188.
- Bitencourt, Cezar. R. (2012).** *Tratado de Direito Penal, Parte Geral*. São Paulo: Editora Saraiva, ed. 17, 2012.
- Bix, Brian H. (2012).** *Contract Law*, New York: Cambridge University Press 2012.
- Blok, P.H. (ed.), (2010).** *Overeenkomsten inzake informatietechnologie*, 2nd ed., The Hague: Sdu 2010.
- Blythe, Stephen E. (2005).** 'Contractual liability of suppliers of defective software: a comparison of the law of the United Kingdom and United States', *Northwestern Journal of International Law & Business* 2005, Volume 26, Issue 1, p. 77-94.
- Boliek, Babette E.L. (2011).** 'FCC Regulation versus Antitrust: How Net Neutrality Is Defining The Boundaries', *Boston College Law Review* 2011, Volume 52, Issue 5, p. 1627-1686.

- Borgesius, F.J. Zuiderveen (2011).** 'De meldplicht voor datalekken in de Telecommunicatiewet', *Computerrecht* 2011, Issue 4, p. 209-218.
- Brennan, Lorin (2000).** 'Why Article 2 Cannot Apply To Software Transactions', *Duquesne Law Review* 2000, Volume 38, Issue 2, p. 459-589.
- Brenner, Susan W. (2004a).** 'Toward a criminal law for cyberspace: product liability and other issues', *Pittsburgh Journal of Technology Law & Policy* 2004, Volume 5, p. [i]-112.
- Brenner, Susan W. (2004b).** 'Distributed Security: Moving Away From Reactive Law Enforcement', *International Journal of Communications Law & Policy*, Available at SSRN: <http://ssrn.com/abstract=623283>.
- Brenner, Susan W. & Clarke, Leo L. (2005).** 'Distributed Security: A New Model of Law Enforcement', Available at SSRN: <http://ssrn.com/abstract=845085>. See also 'Distributed Security: Preventing Cybercrime', *John Marshall Journal of Information Technology & Privacy Law* 2005, Volume 23, Issue 4, p. 659-710, available at <http://repository.jmls.edu/cgi/view-content.cgi?article=1070&context=jitpl>.
- Bridges, Lloyd (2008).** 'The Changing Face of Malware', *Network Security* 2008, Volume 2008, Issue 1, p. 17-20.
- Bubelová, Kamila (2010).** 'Dobré mravy v judikatuře Ústavního soudu ČR', *Právní fórum* 2010, Issue 1, p. 1-7.
- Burstein, Aaron (2003).** 'A Survey of Cybercrime in the United States', *Berkeley Technology Law Journal* 2003, Volume 18, Issue 1, p. 313-338.
- Bygrave, Lee A. & Bing, Jon (2009).** *Internet Governance, Infrastructure and Institutions*, Oxford: Oxford University Press 2009.
- Cardi, W. Jonathan & Green, Michael D. (2008).** 'Duty Wars', *Southern California Law Review* 2008, Volume 81, Issue 4, p. 671-734.
- Carle, J. C. & Perritt H. H. Jr. (2006).** 'Civil liability on the internet', *GPSolo Magazine* 2006, Volume 23, Issue 1, p. 44-47.
- Carroll, Jacob J. (2003).** 'Federal and California Criminal Violations for Distributed Denial-of-Service Transmissions', *UCLA Journal of Law & Technology* 2003, Notes 6, available at http://www.lawtechjournal.com/notes/2003/06_030727_carroll.php
- Carver, Brian W. (2005).** 'Share and Share Alike: Understanding and Enforcing Open Source and Free Software Licenses', *Berkeley Technology Law Journal* 2005, Volume 20, Issue 1, p. 443-481.
- Cavaliere Filho, Sérgio. (2003).** 'Responsabilidade Civil no Novo Código Civil', *Revista da Escola de Magistratura do Rio de Janeiro* 2003, Volume 6, Issue 24, p. 31-47. Available at: http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista24/revista24_31.pdf
- Chandler, Jennifer A. (2004).** 'Security in Cyberspace: Combatting Distributed Denial of Service Attacks', *University of Ottawa Law & Technology Journal* 2004, Volume 1, p. 231-261.

Cheung, Anne S.Y. (2009). 'A study of cyber-violence and internet service providers liability: lessons from China', *Pacific Rim Law & Policy Journal Association* 2009, Volume 18, Issue 2, p. 323-346.

Childers, Seldon J. (2008). 'Don't stop the music: no strict products liability for embedded software', *University of Florida Journal of Law & Public Policy* 2008, Volume 19, Issue 1, p. 125-184.

Chong, Jane (2013a). 'Bad Code: Should Software Makers Pay?', *New Republic* October 3, 2013, available at <http://www.newrepublic.com/article/114973/bad-code-should-software-makers-pay-part-1>

Chong, Jane (2013b). 'Why Is Our Cybersecurity So Insecure?', *New Republic* October 11, 2013, available at <http://www.newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Chong, Jane (2013c). 'What You Don't Know About Internet Security Will Definitely Hurt You', *New Republic* October 22, 2013, available at <http://www.newrepublic.com/article/115281/what-you-dont-know-about-internet-security-will-definitely-hurt-you>

Chong, Jane (2013d). 'We Need Strict Laws If We Want More Secure Software', *New Republic* October 30, 2013, available at <http://www.newrepublic.com/article/115402/sad-state-software-liability-law-bad-code-part-4>

Clark, David S. & Ansay, T. (2002). *Introduction to the law of the United States*, The Hague – London – New York: Kluwer Law International 2002.

Clark, David S. (2002). 'The American Legal System and Legal Culture' in: David S. Clark & T. Ansay, *Introduction to the law of the United States*, The Hague – London – New York: Kluwer Law International 2002, p. 13-34.

Constantin, Lucian (2014). '5 Things You Need to Know About Cybersecurity Insurance', April 25, 2014, available at <http://www.cio.com/article/2376802/security0/5-things-you-need-to-know-about-cybersecurity-insurance.html>.

Coplan, Daniel J. Esq. (2001). 'When is best efforts really best efforts: an analysis of the obligation to exploit in entertainment licensing agreements and a overview of how the term best efforts has been construed in litigation', *Southwestern University Law Review* 2001, Volume 31, Issue 4, p. 725-736.

Cronin, Kevin (2010). 'Best practices and the state of information security', *Chicago-Kent Law Review* 2010, Volume 84, Issue 3, p. 811-819.

Dalsen, W. (2009). 'Civil Remedies for invasions of privacy: a perspective on software vendors and intrusion upon seclusion', *Wisconsin Law Review* 2009, Volume 2009, Issue 4, p. 1059-1092.

Dam, C.C. van (2013). *European Tort Law*, 2nd. Ed, Oxford: Oxford University Press 2013.

De Villiers, Meiring (2004). 'Computer viruses and civil liability: a conceptual framework', *Tort trial & Insurance practice law journal* 2004, Volume 40, Issue 1, p. 123-180.

De Villiers, Meiring (2005). 'Free radicals in cyberspace, complex liability issues in information warfare', *Northwestern Journal of Technology and Intellectual Property* 2005, Volume 4, Issue 1, p. 13-60.

Deflem, M. & Shutt, J. Eagle (2005). 'Law enforcement and computer security threats and measures', May 27, 2005, available at: <https://dumitrudumbrava.files.wordpress.com/2012/01/law-enforcement-and-computer-security-threats-and-measures.pdf>

Dekker, D.F.P. & Van der Linden-Smith, M. (2014). 'De positie van tussenpersonen in Internetcommunicatie', in: Van der Hof, Lodder & Zwenne 2014, p. 261-284.

Dickens, Robert Lee (2007). 'Finding common ground in the world of electronic contracts: the consistency of legal reasoning in clickwrap licenses', *Marquette Intellectual Property Law Review* 2007, Volume 11, Issue 2, p. 379-412.

DLA Piper (2009). *EU study on the Legal analysis of a Single Market for the Information Society - New rules for a new age?* Part 6: *Liability for On-line Intermediaries*. Available at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=835.

Dobbs, Dan B. (2000). *The Law of Torts*, St. Paul (Minn.): West Group 2000.

Dommering-Van Rongen, L. (2000). *Productaansprakelijkheid. Een rechtsvergelijkend overzicht*, Deventer: Kluwer 2000.

Drion, C.E. & de Wit, P. (2005). 'De Service Level Agreement: een bijzondere overeenkomst?', *Contracteren* 2005, Issue 2, p. 32-38.

Earl, Amanda Albrecht (2009). 'Copyright Infringement and Open Source Public Licenses: Jacobsen v Katzer, 535 F.3D 1373 (Fed.Cir. 2008)', *University of Cincinnati Law Review* 2009, Volume 77, Issue 4, p. 1605-1625.

Eeten, M. J. van, Bauer, J.M. Asghari, H., & Tabatabaie, S. (2010). 'The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data', OECD Science, Technology and Industry Working Papers, 2010/05, OECD Publishing. Available at <http://dx.doi.org/10.1787/5km4k7m9n3vj-en>.

Efing, Carlos. (2000). 'O Código de Defesa do Consumidor e os problemas causados pelo bug do ano 2000', in Figueira Júnior, J. Dias & Stoco, R. (2000). *Responsabilidade civil do fabricante e intermediários por defeitos de equipamentos e programas de informática*. São Paulo: Revista dos Tribunais, 2000.

Eijk, N.A.M. van, a.o. (2010). *Moving towards balance: a study into duties of care on the internet*, available at <http://hdl.handle.net/11245/2.95947>, translation of Dutch report *Op weg naar evenwicht: een onderzoek naar zorgplichten op internet*, WODC-report 1854. Available at <http://wodc.nl/onderzoeksdatabase/zorgplicht-internet-service-providers-isps.aspx?cp=44&cs=6796>

Eliáš, Karel et al. (2012). *Nový občanský zákoník s aktualizovanou důvodovou zprávou a rejstříkem*, Ostrava: Sagit 2012.

- ENISA (2011).** 'Botnets: Measurement, Detection, Disinfection and Defence', available at <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/botnets/botnets-measurement-detection-disinfection-and-defence>.
- Farnsworth, E Allan (2004).** *Farnsworth on contracts*, New York: Aspen Publishers 2004, Volume 1, 2 and 3.
- Farnsworth, E. Allan (2010).** *An introduction to the legal system of the United States*, Oxford: University Press 2010.
- Fekete, Imrich (2011).** *Občiansky zákonník: veľký komentár*, Bratislava: EuroKódex 2011.
- Field, Brandi (2010).** 'Net Neutrality: An Architectural Problem In Search Of A Political Solution', *Asper Review of International Business & Trade Law* 2010, Volume 10, p. 187-211.
- Finch, Brian E. & Spiegel, Leslie H. (2014).** 'Litigation following a cyber attack: possible outcomes and mitigation strategies utilizing the safety act', *Santa Clara High Tech Law Journal* 2014, Volume 30, Issue 3, p. 349-374.
- Frazer, Brad (2009).** 'Open Source is not Public Domain: Evolving Licensing Philosophies', *Idaho Law Review* 2009, Volume 45, Issue 2, p. 349-375.
- Gallardo, Claudio Ruiz & Gálvez, Juan Carlos Lara (2011).** *Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America*, available at http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf, see also <http://cyberlaw.stanford.edu/page/wilmap-chile>.
- Giesen, I. (2004).** *Aansprakelijkheid na een nalaten*, Studiekring Offerhaus, nieuwe reeks, nr. 8, Deventer: Kluwer 2004.
- Girot, Clarisse (2001).** *User Protection in IT Contracts*, diss. Tilburg, The Hague: Kluwer Law International 2001.
- Gijrath, S.J.H. (2012).** 'Informatie- en netwerkbeveiliging in juridisch perspectief: een kwestie van contractbesturing', *Computerrecht* 2012/181, Issue 6, p. 382-396.
- Gijrath, S.J.H. & Knol, P.C. (2014).** *Inleiding Telecommunicatierecht*, The Hague: Sdu 2014.
- Glannon, Joseph W. (2005).** *The law of torts*, New York: Aspen Publishers 2005.
- Gold, Steve (2009).** 'The Changing Face of Malware', *Computer Fraud & Security* 2009, Volume 2009, Issue 9, p. 12-14.
- Graaf, T. de (2006).** *Exoneraties in (ICT-)contracten tussen professionele partijen*, Deventer: Kluwer 2006.
- Graaf, T. de & Stuurman, C. (2014).** 'ICT-contracten', in: Van der Hof, Lodder & Zwenne 2014, p. 65-92.
- Gray, D., Citron, D.K. & Rinehart, L.C. (2013).** 'Fighting Cybercrime after United States v. Jones', *Journal of Criminal Law and Criminology* 2013, Volume 103, Issue 3, p. 745-802.
- Gringras, C. (1996).** 'The validity of shrink-wrap licenses', *International journal of Law and information technology* 1996, Volume 4, Issue 2, p. 77-107.

- Gripman, David L. (1997).** 'The doors are Locked but the Thieves and Vandals are Still Getting in: A proposal in tort to alleviate corporate America's cyber-crime problem', *Computer and Information Law* 1997, Volume 16, Issue 1, p. 167-195.
- Guarino, Elizabeth Toni (2002).** 'Chapter Thirty-six: USA' in: Kurer *et al.* 2002, p. 567-588.
- Hamilton, S.N.** 'Made in Canada: A Unique Approach to Internet Service Provider Liability and Copyright Infringement', available at: https://www.irwinlaw.com/sites/default/files/attached/Two_07_Hamilton.pdf
- Handlar, Jiří (2009).** 'Vzdání se práv, která mohou v budoucnu teprve vzniknout, podle § 574 odst. 2 ObčZ', *Právní rozhledy* 2009, Issue 18, p. 659-663.
- Harašta, Jakub (2013).** 'Právní aspekty kybernetické bezpečnosti ČR', *Revue pro právo a technologii* 2013, Issue 8, p. 64-93.
- Harper, J. (2005).** 'Against ISP Liability, Do ISPs have a duty to protect the world?', *Regulation* 2005, Volume 28, Issue 1, p. 30-33.
- Hartkamp, A.S. & Sieburgh, C.H. (2012).** *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel I. De verbintenis in het algemeen, eerste gedeelte*, 14th ed., Deventer: Kluwer 2012.
- Hartkamp, A.S. & Sieburgh, C.H. (2014).** *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel III. Algemeen overeenkomstenrecht*, Deventer: Kluwer 2014.
- Henderson, Stephen E. & Yarbrough, Matthew E. (2002).** 'Suing the insecure? A duty of care in cyberspace', *New Mexico Law Review* 2002, Volume 32, Issue 1, p. 11-25.
- Hendrikse, M.L. & Rinkes, J.G.J. (eds.) (2012).** *Naar een (doorlopende) generieke zorgplicht voor verzekeraars en verzekeringstussenpersonen?*, Volume 10 ACIS-series, Zutphen: Uitgeverij Paris 2012.
- Herdová, Eva (2009).** 'Co přináší nový trestní zákoník', at: <http://www.epravo.cz/top/clanky/co-prinasi-novy-trestni-zakonik-55564.html>.
- Heron, Simon (2007).** 'Botnet command and control techniques', *Network Security* 2007, Volume 2007, Issue 4, p. 13-16.
- Hillman, Robert A. & O'Rourke, Maureen (2009).** 'Rethinking Consideration in the Electronic Age', *Hastings Law Journal* 2009, Volume 61, Issue 2, p. 311-336, also Cornell Law Faculty Working Papers, Paper 48, 2009. Available at http://scholarship.law.cornell.edu/clsops_papers/48
- Hillman, Robert A. & O'Rourke, Maureen (2010).** 'Principles of the Law of Software Contracts: Some Highlights', *Tulane Law Review* 2010, Volume 84, Issue 6, p. 1519-1539.
- Hironaka, Giselda (2007).** 'Responsabilidade Pressuposta: Evolução de Fundamentos e de Paradigmas da Responsabilidade Civil na Contemporaneidade', *Revista da Faculdade de Direito da UFC* 2007, Volume 31, Issue 1, p. 33-59. Available at: <http://www.revistas.ufg.br/index.php/revfd/article/view/12029/7983>

- Hof, S. van der, Lodder, A.R. & Zwenne, G.J. (eds.) (2014).** *Recht en computer*, 6th ed., Deventer: Kluwer 2014.
- Horowitz, Bonna Lynn (1985).** 'Computer Software as a Good under the Uniform Commercial Code: Taking a Byte Out of the Intangibility Myth', *Boston University Law Review* 1985, Volume 65, Issue 1, p. 129-164.
- Hua, Jerry Jie (2014).** 'Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation', *National Taiwan University Law Review* 2014, Volume 9, Issue 1, p. 1-47.
- Hypponen, Mikko (2006).** 'Malware goes mobile', *Scientific American* 2006, p. 70-77, available at http://www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf.
- ITU (2011).** *Understanding Cybercrime: Phenomena, Challenges and Legal Responses*, 2nd ed., draft March 2011. Available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf.
- Jacobs, B. (2013).** 'Ontsluiten door Afsluiten', *Nederlands Juristenblad* 2013, Volume 32, p. 2191-2195.
- Jansa, Lukáš & Otevřel, Petr (2014).** *Softwarové právo*, Brno: Computer Press 2014.
- Joerling, Jill (2010).** 'Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data', *Washington University Journal of Law & Policy* 2010, Volume 32, Issue 1, p. 467-488.
- Jong, G.T. de (2006).** *Niet-nakoming van verbintenissen*, Monografieën BW B33, Deventer: Kluwer 2006.
- Kaspersky Lab (2014).** *Global IT security risks survey 2014 – Distributed Denial of Service (DDoS) Attacks*. Available at <https://press.kaspersky.com/files/2014/11/B2B-International-2014-Survey-DDoS-Summary-Report.pdf>.
- Keeton, W. Page, Dobbs, Dan B., Keeton, Robert E. & Owen, David G. (1984).** *Prosser and Keeton on Torts*, 5th ed., St. Paul (Minn.): West Publishing 1984.
- Kim, C., Newberger, B. & Shack, B. (2012).** 'Computer Crimes', *American Criminal Law Review* 2012, Volume 49, Issue 2, p. 443-488.
- Knebl 2010.** 'Odpovědnost za vady software', *Právní rádce*, available at: <http://pravniradce.ihned.cz/c1-46529960-odpovednost-za-vady-software>.
- Kooijmans, T., Tjong Tjin Tai, T.F.E. & Waard, B.W.N. de (2014).** *Het gebruik van onderzoeksinformatie en rapporten van de Onderzoeksraad voor veiligheid in juridische procedures*, Tilburg. Available at: http://www.onderzoeksraad.nl/uploads/fm/Universiteit%20van%20Tilburg/Rapport_2014_definitief.pdf
- Koops, B.J. (red.) (2007).** *Strafrecht en ICT*, 2nd ed., The Hague: Sdu 2007.
- Koops, B.J. (2010).** 'Cybercrime Legislation in the Netherlands', Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes', available at <http://ssrn.com/abstract=1633958>
- Koops, B.J. (2014).** 'Cybercriminaliteit', in: Van der Hof, Lodder & Zwenne 2014, p. 213-242.

- Kopf, K.A. (1987).** 'Warranties and Commercial Supply Contracts: A Need for Definitive Rules', *Public Contract Law Journal* 1987, Volume 17, Issue 2, p. 534-552.
- Korbel, František (2012).** Dnes vyšel nový občanský zákoník, Blog Jiné právo, available at: <http://jinepravo.blogspot.nl/2012/03/frantisek-korbel-dnes-vysel-novy.html> [accessed: 1 December 2014].
- Kortmann, J. S. (2005).** *Altruism in Private Law*, Oxford: Oxford University Press 2005.
- Kratochvíl, Vladimír (2012).** *Trestní právo hmotné: obecná část*, Praha: C.H. Beck 2012.
- Kruijer, H.S.M. (2000).** *De exonerationclausules in de algemene voorwaarden van de Federatie van Nederlandse ondernemingen in de informatietechnologie (FENIT)*, Deventer: Kluwer 2000.
- Kurer, M., Codoni, S., Günther, K., Santiago Neves, J. & Teh, L. (eds.) (2002).** *Warranties and Disclaimers. Limitation of Liability in Consumer-Related Transactions*, London: Kluwer Law International 2002.
- Kuwahara, Emily (2007).** 'Torts v. Contracts: can Microsoft be held liable to home consumers for its security flaws?', *Southern California Law Review* 2007, Volume 80, Issue 5, p. 997-1037.
- La Rue, F. (2011).** 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', United Nations Human Rights Council, New York, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Lannetti, David W. (2000).** 'Toward a Revised Definition of "Product" under The Restatement (Third) of Torts: Product Liability', *Tort & Insurance Law Journal* 2000, Volume 35, Issue 4, p. 845-889.
- Lazar, Jan (2010).** *Občianske právo hmotné I*, Bratislava: Iura edition 2010.
- Leonardi, Marcelo (2005).** Responsabilidade Civil dos Provedores de Serviço da Internet, 2005. Available at: <http://leonardi.adv.br/wp-content/uploads/2011/04/mlrcpsi.pdf>
- Levy, Lawrence B. & Bell, Suzanne Y. (1990).** 'Software product liability: understanding and minimizing the risks', *High Technology Law Journal* 1990, Volume 5, Issue 1, p. 1-27. Available at <http://www.law.berkeley.edu/journals/btlj/articles/vol5/Levy/html/text.html>
- Lichtman, D. (2004-2005).** 'Holding Internet Service Providers Accountable', *Regulation* 2004-2005, Volume 27, Issue 4, p. 54-59.
- Lichtman, D. & Posner, E. (2004).** Holding Internet Service Providers Accountable, the law school the University of Chicago, July 2004, http://ssrn.com/abstract_id=573502.
- Lichtman, D. & Posner, E. (2006).** 'Holding Internet Service Providers Accountable', *Supreme Court Economic Review* 2006, Volume 14, p. 221-260.
- Luo, X. & Liao, Q. (2007).** 'Awareness Education as the Key to Ransomware Prevention', *Information Systems Security* 2007, Volume 16, Issue 4, p. 195-202.
- MacCarthy, Mark (2010).** 'What Payment Intermediaries Are Doing About Online Liability and Why It Matters', *Berkeley Technology Law Journal* 2010, Volume 25, Issue 2, p. 1037-1120.

Machado, Alexandre Mattos and Inês, Maria Alice de Oliveira Santa (2012). 'A exceptio non adimpleti contractus e a possibilidade jurídica da cláusula solve et repete', *Revista de Direito da UNIFACS*, issue 139. Available at <http://www.revistas.unifacs.br/index.php/redu/article/viewFile/1879/1428>.

Maisner, Martin et al. (2011). *Základy softwarového práva*, Praha: Wolters Kluwer 2011.

Mann, Ronald J. & Belzley, Seth R. (2005). 'The Promise of Internet Intermediary Liability', *William and Mary Law Review* 2005, Volume 47, Issue 1, p. 239-307.

Martin, A.K. & Andrade, N.N.G. de (2012). 'Battling Botnets with Digital Rights in Mind', *European Journal for Law and Technology* 2012, Volume 3, No. 2, available at <http://ejlt.org/article/view/158/238>

Martins, Guilherme M. (2014). *Responsabilidade Civil por Acidentes de Consumo na Internet*. Rio de Janeiro: Revista dos Tribunais, ed. 2, 2014.

Materna, Mark G. (2012). 'Protecting Generation Z: A brief policy argument advocating vicarious liability for Internet Service Providers', *University of San Fransisco Law Review* 2012, Volume 47, Issue 1, p. 109-132.

McLaurin, Joshua (2011). 'Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks', *Yale Law & Policy Review*, Volume 30, Issue 1, p. 211-254.

Meehan, Shea C. (2000). 'Consumer protection law and the uniform electronic transactions act (UETA): why states should adopt UETA as drafted', *Idaho Law Review* 2000, Volume 36, Issue 3, p. 563-584.

Mehra, S.K. (2010). 'Law and Cybercrime in the United States Today', *The American Journal of Comparative Law Supplement* 2010, Volume 58, p. 659-686.

Mehren, Taylor von (1988). *Law in the United States*, Deventer – Antwerp – London – Frankfurt – Boston – New York: Kluwer Law and Taxation Publishers 1988.

Meulen, N.S. van der & Lodder, A.R. (2014). 'Cybersecurity', in: Van der Hof, Lodder & Zwenne 2014, p. 301-318.

Meurkens, R.C. (2014). Punitive Damages. *The Civil Remedy in American Law, Lessons and Caveats for Continental Europe*, Deventer: Kluwer 2014.

Moore, Tyler (2010). 'Introducing the Economics of Cybersecurity: Principles and Policy Options', Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, available at <http://www.nap.edu/catalog/12997.html>.
Moringiello, Juliet M. & Reynolds, William L. (2010). 'What's Software Got To Do with It? The ALI Principles of the Law of Software Contracts', *Tulane Law Review* 2010, Volume 84, Issue 6, p. 1541-1556.

Morrison, Steven R. (2011). 'What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents', *Virginia Journal of Law & Technology* 2011, Volume 16, Issue 2, p. 253-300.

- Mueller, Lance (2006).** 'Webjacking, and how to boot it out', *Network Security* 2006, Volume 2006, Issue 8, p. 15-18.
- Murtagh, Michael P. (2009).** 'The FCC, the DMCA, and Why Takedown Notices Are Not Enough', *Hastings Law Journal* 2009, Volume 61, Issue 1, p. 233-274.
- NCSC (2014).** *Cyber Security Assessment Netherlands 4*, available at <https://www.ncsc.nl/english/current-topics/news/cyber-security-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat.html>
- NCTV (2011).** *Juridisch kader Cyber Security*, The Hague. Available at <https://zoek.officielebekendmakingen.nl/blg-147059>
- NCTV (2013).** *Nationale Cybersecurity Strategie 2*, The Hague. Available at <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2.html>
- Net, C.B. van der (2000).** *Grenzen stellen op internet. Aansprakelijkheid van Internetproviders en rechtsmacht*, PhD thesis Leiden, Deventer: Kluwer 2000.
- Novotný, Oto, Vokoun, Rudolf, Šámal, Pavel et al.(2010).** *Trestní právo hmotné. Zvláštní část*, Praha : Wolters Kluwer 2010.
- OECD (2008).** *Malicious Software (Malware): A Security Threat to the Internet Economy*, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, available at <http://www.oecd.org/internet/ieconomy/40724457.pdf>
- OECD (2009).** *Computer Viruses and Other Malicious Software. A Threat to the Internet Economy*, OECD Publishing. Available online at http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en
- OECD (2012a).** *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies*, available at <http://oe.cd/cybersecurity-strategies>
- OECD (2012b).** "Proactive Policy Measures by Internet Service Providers against Botnets", OECD Digital Economy Papers, No. 199, OECD Publishing. Available at <http://dx.doi.org/10.1787/5k98tq42t18w-en>.
- Ommeren, F.J. van (2011).** 'Zorgplichten: wat zijn dat? Een poging tot overbrugging van twee werelden', in: C.E.C. Jansen, S.A.J. Munneke, F.J. van Ommeren & J.W. Rutgers (eds.), *Zorgplichten in publiek- en privaatrecht*, Den Haag, Boom Juridische uitgevers, p. 23-45.
- Oswald, E. (2006). Ransomware Becoming a Serious Problem. BetaNews, July 24, 2006. Available at http://www.betanews.com/article/Ransomware_Becoming_a_Serious_Problem/1153780370
- Otto, P.N. (2009).** 'Reasonableness Meets Requirements: Regulating Security and Privacy in Software', *Duke Law Journal* 2009, Volume 59, Issue 2, p. 309-342.

- Pannetrat, A. (2011).** In the privacy of botnet communications, presentation for workshop Botnets, Measurement, Detection, Disinfection and Defence, available at <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/presentations-from-the-workshop-botnets-measurement-detection-disinfection-and-defence>.
- Pasqualotto, Adalberto de S. (2002).** 'Princípios Básicos do Direito Contratual no Novo Código Civil', *Anais do EMERJ Debate o Novo Código Civil* 2002, p. 219-235. Available at: http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/anais_onovocodigocivil/anais_especial_1/Anais_Parte_I_revistaemerj_219.pdf
- Peters, Rachael M. (2014).** 'So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws', *Arizona Law Review* 2014, Volume 56, Issue 4, p. 1171-1202. Available at <http://www.arizonalawreview.org/pdf/56-4/56arizrev1171.pdf>
- Peterson, J., Segal, L. & Eonas, A. (2014).** 'Global Cyber Intermediary Liability: A Legal and Cultural Strategy', *Pace Law Review* 2014, Volume 34, Issue 2, p. 586-630.
- Pinguelo, F.M., Lee, W. & Muller, B.W. (2012).** 'Virtual Crimes, Real Damages Part II: What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships are Attempting to Achieve for the Nation of Tomorrow', *Virginia Journal of Law & Technology* 2012, Volume 17, issue 1, p. 75-88.
- Pinkney, Kevin R (2002).** 'Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure', *Albany Law Journal of Science & Technology* 2002, Volume 13, Issue 1, p. 43-82.
- Polčák, Radim (2007).** *Právo na internetu: spam a odpovědnost ISP*, Brno: Computer Press 2007.
- Polčák, Radim (2012).** *Internet a proměny práva*, Praha: Auditorium 2012.
- Pouperova, Olga (2013).** 'Update: An Introduction to the Czech Legal System and Legal Resources Online', available at http://www.nyulawglobal.org/Globalex/Czech_Republic1.htm.
- Prins, Corien (2007).** 'Nalaten in Cyberspace', *Nederlands Juristenblad* 2007, Volume 82, Issue 6, p. 321.
- Prins, Corien (2013).** 'Zorgplichten en Cybercrime', *Nederlands Juristenblad* 2013, Volume 88, Issue 18, p. 1185.
- Prins, Corien & Schellekens, M.H.M. (2004).** 'The Chilling-Effect of Liability Law on Initiatives to Enhance the Reliability of On-line Health-Related Information', *European Journal of Health Law* 2004, Volume 11, Issue 2, p. 201-208.
- Prins, Corien & Schellekens, M.H.M. (2005).** 'Fighting untrustworthy Internet content: In search of regulatory scenarios', *Information Polity* 2005, 10, nr. 1, 2, p. 129-139.
- Raaijmakers, G.T.M.J. (2002).** *Garanties bij overnames*, Den Haag: BJU Uitgevers 2002.
- Reitz, John C. & Carlson, J. (2002).** 'Commercial Transactions' in: *Introduction to the law of the United States*, The Hague – London – New York: Kluwer Law International 2002, p. 281-310.

Říha, Jiří (2008). 'Odpovědnost providerů se zaměřením na odpovědnost Host-Providera a Access-Providera', *Acta Universitatis Carolinae Iuridica* 2008, p. 107-129.

Rizzato Nunes, Luiz.A. (2012). *Curso de Direito do Consumidor*. São Paulo: Editora Saraiva, ed. 7, 2012.

Rode, Lilia (2007). 'Data Security Breach Notification Statutes: Does Placing The Responsibility On The True Victim Increase Data Security', *Houston Law Review* 2007, Volume 43, Issue 5, p. 1597-1634.

Rosen, Lawrence (2005). *Open Source Licensing*, New Jersey: Prentice Hall 2005.

Rowe, Brent and others (2011). 'The Role of Internet Service Providers in Cyber Security', Research Brief, Institute for Homeland Security Solutions, available at http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf.

Rustad, Michael L. & Koenig, Thomas H. (2005). 'The tort of Negligent Enablement of Cybercrime', *Berkeley Technology Law Journal* 2005, Volume 20, Issue 4, p. 1553-1611.

Rustad, Michael L. & Onufrio, Maria Vittoria (2010). 'The Exportability of the Principles of Software: Lost in Translation?', *Hastings Science & Technology Law Journal*, Volume 2, p. 25-80. Also available at <http://ssrn.com/abstract=1466875>.

Salim, Adib P. N. (2005). 'A Teoria do Risco Criado e a Responsabilidade Objetiva do Empregador em Acidentes de Trabalho', *Revista do Tribunal Superior do Trabalho 3^{ff} Região* 2005, Volume 41, Issue 71, p. 97-110. Available at: http://www.trt3.jus.br/escola/download/revista/rev_71/Adib_Salim.pdf

Šámal, Pavel et al. (2012). *Trestní zákoník: komentář*, Praha: C.H. Beck 2012.

Santanam, R., Sethumadhavan, M., Virendra, M. (2010). *Cyber Security, Cyber Crime and Cyber Forensics*, Hershey New York: Information Science Reference 2010.

Scala, Caroline S. (2011). 'The FCC's Role in Regulating Network Neutrality: Protection of Online Innovation & Business', *Chapman Law Review* 2011, Volume 51, p. 419-442.

Schermer, B.W. & Lodder, A.R. (2014). 'ICT-contracten', in: Van der Hof, Lodder & Zwenne 2014, p. 1-24.

Schjølberg, Stein & Hubbard, Amanda M. (2005). *Harmonizing National Legal Approaches on Cybercrime*, ITU 2005. Available at http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

Scott, Michael D. (2008). 'Tort liability for vendors of insecure software: has the time finally come?', *Maryland Law Review* 2008, Volume 67, Issue 2, p. 425-484.

Schellekens, M. (2001). *Aansprakelijkheid van Internetaanbieders*, PhD thesis Tilburg, The Hague: SDU 2001.

Schreiber, Anderson (2009). *Novos Paradigmas da Responsabilidade Civil*. São Paulo: Atlas, ed. 2, 2009.

Schwartz, Paul M. & Janger, Edward J. (2007). 'Notification of Data Security Breaches', *Michigan Law Review* 2007, Volume 105, Issue 5, p. 913-984.

- Sembhi, Sarb (2013).** 'An introduction to cyber liability insurance cover', Computerworld, available at <http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover>.
- Sergienko, Gregory S. (2006).** 'Assumption of Risk As a Defense to Negligence', *Western State University Law Review* 2006, Volume 34, Issue 1, p. 1-28.
- Shah, Pratik A. (2000).** 'The Uniform Computer Information Transactions Act', *Berkeley Technology Law Journal* 2000, Volume 15, issue 1, p. 85-108.
- Shaw, Abraham (2010).** 'Data Breach: From Notification to Prevention Using PCI DSS', *Columbia Journal of Law and Social Problems* 2010, Volume 43, Issue 4, p. 517-562.
- Sherling, M. (2014).** 'The likely regulators? An analysis of FCC jurisdiction over cyber-security', *Federal Communications Law Journal* 2014, Volume 66, Issue 3, p. 569-608.
- Siemerink, L.A.R. (2007).** *De overeenkomst van Internet Service Providers met consumenten*, PhD thesis Leiden, Deventer: Kluwer 2007.
- da Silva Pereira, Caio M. (2013).** *Instituições de Direito Civil*, vol. 3, Rio de Janeiro: Forense, ed. 17, 2013.
- Sinrod, Eric J. & Reilly, William P. (2000).** 'Cyber-crimes: a practical approach to the application of federal computer crime laws', *Computer High Technology Law Journal* 2000, Volume 16, Issue 2, p. 177-232.
- Smits, Jan M. (2000).** *The Good Samaritan in European Private Law*, Deventer: Kluwer 2000.
- Stamhuis, E.F. (2012).** 'Criminal Law on Cyber Crime in the Netherlands; General Part', AIDP Country Report Section I, Preparatory Colloquium Verona (Italy), 28 – 30 November 2012, available at <http://www.penal.org/sites/default/files/files/RV-11.pdf>.
- Stuber, Walter D. & Belluomini, Márcio (2002).** 'Chapter Nine: Brazil', in: Kurer *et al.* (2002), p. 133-147.
- Sulkowski, Adam J. (2007).** 'Cyber-Extortion: Duties and Liabilities related to the Elephant in the Server Room', *University of Illinois Journal of Law Technology & Policy* 2007, Volume 2007, Issue 1, p. 21-63.
- Sunstein, Cass R. (1999).** 'Information Regulation and Information Standing: Akins and Beyond', *University of Pennsylvania Law Review* 1999, Volume 147, Issue 3, p. 613-675.
- Svajcer, Vanja (2012).** *When Malware Goes Mobile: Causes, Outcomes and Cures*, Sophos Whitepaper, available at http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/Sophos_Malware_Goes_Mobile.pdf?la=en.pdf
- Švestka, Jiří et al. (2013).** *Občanský zákoník: komentář*. 1. sv., Praha: Wolters Kluwer 2013.
- Švestka, Jiří et al. (2013).** *Občanský zákoník: komentář*. 6. sv., Praha: Wolters Kluwer 2013.
- Swire, Peter P. (2005).** 'Elephants and mice revisited: law and choice of law on the internet', *University of Pennsylvania Law Review* 2005, Volume 153, Issue 6, p. 1975-2001.
- Táborová, Alice (2010).** 'Veřejnoprávní ochrana informační společnosti a místní působnost práva', *Revue pro právo a technologii*, 2010, Issue 1, p. 29-60.

- Tartuce, Flávio (2014).** *Direito Civil – Teoria Geral das Obrigações e Contratos*, vol. 2. São Paulo: Método, ed. 9, 2014.
- Tartuce, Flávio & Neves, Carlos. (2014).** *Manual de Direito do Consumidor. Direito Material e Processual*. São Paulo: Método, ed. 3, 2014.
- Taskovska, D. (2010).** 'General Principles as sources of law in the major contemporary legal systems', *Iustinianus Primus Law Review* 2010, available at <http://www.law-review.mk/pdf/01/Dobrinka%20Taskovska.pdf>.
- Tepedino, Gustavo (2012).** Novos Princípios Contratuais e Teoria da Confiança: a exegese da cláusula to the best knowledge of the sellers. Available at: <http://www.tepedino.adv.br/wp/wp-content/uploads/2012/09/biblioteca13.pdf>
- Tettenborn, A. (2008).** 'What it's worth to do your best', *Pace Law Review* 2008, Volume 28, Issue 2, p. 297-314.
- Tichý, Luboš (2004).** 'Contributory Negligence under Czech Law' in: Magnus, Ulrich and Martín-Casals eds. (2004). *Unification of Tort Law: Contributory Negligence*, The Hague: Kluwer Law International 2004.
- Timmer, W. (2011).** *Het doel wel gesteld. Een praktijkonderzoek naar de toepassing van doelregelgeving* (diss. Rotterdam), Den Haag: Boom Juridische uitgevers 2011.
- Timmer, W. (2013).** 'Zorgplichten aan het werk', *Regelmaat*, p. 354-366.
- Tjong Tjin Tai, T.F.E. (2004a).** 'Toerekenbare niet-nakoming en de zorg van een goed schuldenaar', *Weekblad voor Privaatrecht, Notariaat en Registratie* 2004, 6574, p. 285-290.
- Tjong Tjin Tai, T.F.E. (2004b).** 'Garantie, nakoming en schadevergoeding', *Weekblad voor Privaatrecht, Notariaat en Registratie* 2004, 6577, p. 363-368.
- Tjong Tjin Tai, T.F.E. (2007a).** *Zorgplichten en zorgethiek*, diss. Amsterdam (UvA), Deventer: Kluwer 2007.
- Tjong Tjin Tai, T.F.E. (2007b).** 'Nalaten als onrechtmatige daad', *Nederlands Juristenblad* 2007, 40, p. 2540-2546.
- Tjong Tjin Tai, T.F.E. (2010).** 'Zorg, privaatrecht en publiekrecht: van ondersteuning naar handhaving, en terug', *Recht der Werkelijkheid* 2010, Volume 31, nr. 3, p. 6-25.
- Tjong Tjin Tai, T.F.E. (2011).** Ch. 17 'Duties of Care and Ethics of Care. A Case Study in Law and Ethics', in: *Law and Method*, eds. S. Taekema & B. van Klink, Tübingen: Mohr Siebeck 2011, p. 329-340.
- Tjong Tjin Tai, T.F.E. (2012).** 'Generieke zorgplicht in theorie en praktijk', in: M.L. Hendrikse, J.G.J. Rinkes (red.), *Naar een (doorlopende) generieke zorgplicht voor verzekeraars en verzekeringstussenpersonen?*, ACIS-serie dl. 10, Zutphen: Paris 2012, p. 37-49.
- Tjong Tjin Tai, T.F.E. (2013).** 'Zorgplichten van banken tegen DDoS-aanvallen', *Nederlands Juristenblad* 2013, Volume 88, p. 2196-2200.

Tjong Tjin Tai, T.F.E. (2015). 'Professional Diligence as a Standard in European Private Law', Available at <http://ssrn.com/abstract=2565877>.

Tomasevicius Filho, Eduardo (2013). 'Good Faith in the Brazilian Civil Code: Ten Years Later', *Teisės aktualijos* 2013, Volume 88, p. 211-221. Available at: <http://www.zurnalai.vu.lt/files/journals/5/articles/1604/public/211-221.pdf>

Tomíšek, Jan (2014). 'Software jako věc v režimu nového občanského zákoníku', *Revue pro právo a technologii* 2014, p. 199-212.

Tonkelaar, J.D.A. den (1982). *Resultaatsverbintenissen en inspanningsverbintenissen*, Zwolle: W.E.J. Tjeenk Willink 1982.

UNODC (2013). *Comprehensive Study on Cybercrime*, draft, February 2013. Available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBER-CRIME_STUDY_210213.pdf

Venosa, Sílvio de S. (2013). *Teoria Geral das Obrigações e dos Contratos*, vol. 2. São Paulo: Atlas, ed. 13, 2013.

Verschuuren, J.M. (1990). 'Wettelijke algemene zorgplichten in het milieurecht', in: H.A.M. Backx e.a. (eds.), *Recht doen door wetgeving*, Zwolle: W.E.J. Tjeenk Willink, p. 419-430.

Viney, G. (2008). J. Ghestin, *Traité de droit civil: Introduction à la responsabilité*, 3rd ed., Paris: L.G.D.J. 2008.

Visser, M.J.C. (2001). *Zorgplichtbepalingen in het strafrecht*, Arnhem: Gouda Quint 2001.

Voelzke, J. (2003). 'Don't Shoot: I'm Just the Web Site Host!', *The computer and internet lawyer* 2003, Volume 20, Number 5, p. 4-15.

Wald, Arnaldo & Giancoli, Brunno P. (2012). *Direito Civil*, vol. 7 – Da Responsabilidade Civil. São Paulo: Saraiva, 2012.

Warner, R. & Sloan, Robert H. (2012). 'Vulnerable Software: Product-risk Norms and the Problem of Unauthorized Access', *University of Illinois Journal of Law, Technology & Policy* 2012, Volume 2012, Issue 1, p. 45-94.

Watkins, Casey G. (2013). 'Wireless Liability: liability concerns for operators of unsecured wireless networks', *Rutgers Law Review* 2013, Volume 65, Issue 2, p. 635-665.

Weber, Lori A. (1992). 'Bad Bytes: The Application of Strict Products Liability to Computer Software', *St. John's Law Review* 1992, Volume 66, Issue 2, p. 469-485.

Wessels, B., Jongeneel, R.H.C. & Hendrikse, M.L. (eds.) (2010). *Algemene voorwaarden*, 5th ed., Deventer: Kluwer 2010.

Westerdijk, R.J.J. (1995). *Produktaansprakelijkheid voor software: beschouwingen over de aansprakelijkheid voor informatieproducten*, Deventer: Kluwer.

Winn, Jane K. (2009). 'Are Better Security Breach Notification Laws Possible?', *Berkeley Technology Law Journal* 2009, Volume 24, Issue 3, p. 1133-1166.

Wong, J. (2011). 'Net Neutrality: Preparing for the future', *Journal of the National Association of Administrative Law Judiciary* 2011, Volume 31, Issue 2, p. 669-719.

Zekoll, J. & Fleming, J.G. (2002). 'Torts' in: David S. Clark & T. Ansay, *Introduction to the law of the United States*, The Hague – London – New York: Kluwer Law International 2002, p. 189-207.

Zimmermann, Reinhard & Whittaker, Simon (eds.) (2000). *Good Faith in European Contract Law*, Cambridge: Cambridge University Press 2000.

Ziniti, C. (2008). 'The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it right and web 2.0 proves it', *Berkeley technology law journal* 2008, Volume 23, Issue 1, p. 583-616.

Zitrin, Richard, & Langford, Carol M. (1999). *The Moral Compass of the American Lawyer*, New York: Ballantine 1999.

Zwenne, G.J. & Knol, P.C. (2014). 'Elektronische communicatie', in: Van der Hof, Lodder & Zwenne 2014, p. 143-178.

Annex 2. Legislation and case law

2.1. *Treaties*

Budapest Convention on Cybercrime of 23 November 2001

2.2. *EU legislation and case law*

Legislation

Directive 85/374/EEC

Directive 95/46/EC

Directive 2000/31/EC (art. 12-15, recital 42)

Directive 2002/21/EC of 2002

Directive 2002/58/EC

Directive 2006/24/EC

Directive 2009/136/EC (Cons. 28)

Directive 2013/40/EU of 12 August 2013 (3, 8(1), Cons. 17, 29)

EU Framework Decision 2005/222/JHA

EU Regulation 611/2013

Case law

ECJ 29 January 2008, case C-275/06 (Promusicae/Telefónica)

ECJ 23 March 2010, cases C-236/08-C-238/08 (Google Adwords)

ECJ 12 July 2011, C-324/09 (L'Oréal/eBay)

ECJ 24 November 2011, case C-70/10 (Scarlet Extended/Sabam)

ECJ 16 February 2012, case C-360/10 (SABAM/Netlog)

ECJ 8 April 2014, cases C-293/12 and C-594/12

2.3. *Dutch legislation and case law*

Legislation

Besluit aanwijzing toezichthouders Telecommunicatiewet (2(1))

Besluit continuïteit openbare elektronische communicatienetwerken en diensten, oktober 2012 (1(d))

Dutch Code of Civil procedure (WBRv) (19-22, 843a, 254)

Dutch Civil Code of 1838 (art. 1402)

Dutch Civil Code (BW) (2:1, 3:305a, 3:305b, 6:2, 6:75, 6:106, 6:162, 6:196c, 6:248, 7:17(2), 7:401).

Dutch Criminal Code (WvSr) (23, 45, 47, 48, 54a, 138a-old (138ab), 139d para 2, 161ter,

161sexies, 161 septies, 317 para 2, 326, 350a, 350b, 350d (proposed bill), 351, 351bis, 450)
 Dutch Telecommunication Act (Tw) (1.1(a), 2.1, 7.4a(1)(b)(d), 11a1(2), 2(1), 11.2a, 11.3, 11.3a, 11.5, 13.2a, 15.1, 15.2)
 Wet bescherming persoonsgegevens (Wbp)
 Wet Collectieve Afwikkeling Massaschade (WCAM)
 Wet op de economische delicten

Case law

HR 10 June 1910, W. 9038 (Zutphense juffrouw)
 HR 31 January 1919, W. 10365 (Lindenbaum/Cohen)
 HR 23 February 1954, NJ 1954/378.
 HR 2 December 1966, NJ 1967/42 (Haringkar).
 HR 22 November 1974, NJ 1975/149 (Struikelende broodbezorger).
 HR 13 March 1981, NJ 1981/635 (Ermes/Haviltex).
 HR 27 May 1988, NJ 1989/29 (Veenbroei).
 HR 9 November 1990, NJ 1991/26 (Speeckaert/Gradener).
 HR 4 October 1996, NJ 1997/594.
 HR 25 October 2002, NJ 2004/556 (Paardrijles).
 HR 20 February 2004, NJ 2005/493 (DSM /Fox).
 HR 28 May 2004, NJ 2005/105 (Jetblast).
 HR 25 November 2005, NJ 2009/550 (Lycos/Pessers).
 HR 25 November 2005, NJ 2009/103.
 HR 14 April 2006, NJ 2006/259.
 HR 19 October 2007, NJ 2007/565 (ETC/Vodafone).
 HR 5 June 2009, NJ 2012/182-184 (Effectenlease).
 HR 22 February 2011, ECLI:NL:HR:2011:BN9287.
 HR 27 April 2012, ECLI:NL:HR:2012:BV1301, NJ 2012/293 (Beeldbrigade).
 HR 25 May 2012, NJ 2012/340.

Gerechtshof Amsterdam 22 November 2001, LJN AD7868, Computerrecht 2002/2, p. 94
 (Kirche in Not/Cap Gemini)

2.4. U.S. legislation and case law

Legislation

ALI Principles of the law of software contracts (§ 2.02 (b), § 3.05, § 4.02)
 California Civil Code (§ 1708-1725, 1798)
 California data security breach notification law of 2002
 California Penal Code (502)
 Communications Assistance for Law Enforcement Act
 Communications Decency Act (§ 230)
 Digital Millennium Copyright Act
 Federal Criminal Code (FCC)
 Federal Rules of Civil Procedure (§ 23)
 Federal Wiretap Act
 Health Insurance Portability and Accountability Act 1996 (HIPAA) Breach Notification Rule,
 45 CFR §§ 164.400-414
 Personal Data Notification & Protection Act (proposal)
 Restatement (Second) of Contracts (1981)
 Restatement (Third) of Torts (§ 7(a)) § 19, § 19a)
 Restatement of the Law (Second) Torts (§ 314 + 314A, 356(1), 402A)
 Stored Communications Act
 Uniform Commercial Code (U.C.C.) (art. 1-9, § 2-306-2, 2-313, 2-314, 2-315, 2-316, 2-719)
 Uniform Computer Information Transactions Act (UCITA) (§ 406, 804)
 Uniform Electronic Transactions Act
 17 U.S.C. (§512 (a-d))
 18 U.S.C. (§ 2, 3, 1030, 2510-2522, 2701-2711)
 28 U.S.C. (§ 1332(d), 1453, 1711-1715)
 47 U.S.C. (§ 151, 230 (c)(2), 1001)

Case law

Aas v. Superior Court (William Lyon Company) (2000) 24 Cal.4th 627, 101 Cal.Rptr.2d 718;
 12 P.3d 1125.
 Abdallah v. Caribbean Sec. Agency, 557 F.2d 61, 63 (3d Cir. 1977)
 Azzarello v. Black Bros. Co. 480 Pa. 547 (1978) 391 A.2d 1020.
 Bloor v. Falstaff Brewing Corp 601 F.2d 609 (2d Cir. 1979).
 Cannon v. Sears Roebuck & Co. 1978, 374 Mass. 739, 374 N.E.2d 582.
 Caudill Seed & Warehouse Co. v. Prophet 21, Inc., 123 F. Supp. 2d 826, 829 (E.D. Pa. 2000).
 Chastain v. Fuqua Indust., Inc., 275 S.E.2d 679 (Ga. Ct. App. 1980).
 Dalton v. Educational Testing Serv. 663. N.E.2d 289 (N.Y. 1995)

Dundee Cement Co v. Chemical Labs., 712 F.2d 1166, No. 82-2894 (7th Cir. 1983).

Giggers v. Memhis Hous. , 277 S.W.3d 359, 364. (Tenn. 2009).

Handiboe v. McCarthy, 151 S.E.2d 905 (Ga. Ct. App. 1966)

Jacobsen v. Katzer 535 F.3d 1373 (Fed. Cir. 2008).

Jaire Corp v. Gregor Spagnol Enters., Inc. v. Digital Equip. Corp., 568 A.2d 948, 951–52 (Pa. Super. Ct. 1989)

J'Aire Corp. v. Gregory , 24 Cal.3d 799 S.F. No. 23983, August 13, 1979. Available at <http://scocal.stanford.edu/opinion/jaire-corp-v-gregory-30547>

People Express Airlines v. Consolidated Rail Corp. 100 N.J. 246, 495 A.2d 107 (1985).

ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996)

Richards v. City of Lawton. Okl.1981 629 P.2d 1260.

Rosemond v United States, case no. 12-895, decided 5 March 2014

Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968).

Smith v. Anderson, 72 P.3d 369, 372. (Colo. Ct. App. 2002).

Spagnol Enters., Inc. v. Digital Equip. Corp., 568 A.2d 948, 951–52 (Pa. Super. Ct. 1989).

Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995)

U.S. vs. Ancheta, 06-051 (C.D. Cal.), Febr. 2005 Grand Jury, available at <http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf>.

United States v. Jones, 132 S. Ct. 945 (2012)

Vaughan v. Menlove, 1837, 3 BingN.C. 468, 132 Eng. Rep. 490.

Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014)

Vining v. Avis Rent-A-Car 354 So. 2d 54, 55 (Fla. 1977)).

Wood v. Lucy, Lady Duff-Gordon, 222 N.Y. 88, 118 N.E. 214 (1917).

2.5. Brazilian legislation and case law

Legislation

Brazilian Code of Civil Procedure (333)

Brazilian Criminal Code (13, §2)

Brazilian Software Act (10, §1, II of Law 9.609/1988)

Brazilian Civil Code (BrCC) (112, 113, 186, 187, 188, 206, 233-242, 243-246, 247-249, 250-251, 389-393, 421, 422, 476, 927, 930, 931, 932, 945, 2035)

Brazilian Code of Consumer Defence (BrCDC) (1, 2, 4, 6, 8, 12, 14, 18, 19, 20, 24, 26, 27, 38, 51, 81, 87)

Brazilian Civil Code of 1916

Law 7.347/1985 (1, 5)

Federal Constitution, art. 5, inc. LXXIV

Marco Civil da Internet (Law 12.096/2014) (3, I to VI, art. 9, 10, 18 to 21)

Presidential Decree 7.692/2013

Telecommunications Act (Law 9.472/1997)

2.6. Czech legislation and case law

Legislation

Předpis č. 316/2014 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti / Cybersecurity Notice.

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod / Bill of Fundamental Rights and Freedoms (art. 7(1), 10(2), 13)

Zákon č. 141/1961 Sb., trestní řád (TrŘ) / Code of Criminal Procedure (2(3))

Zákon č. 99/1963 Sb., občanský soudní řád (OSŘ) / Code of Civil Procedure (159a(2))

Zákon č. 40/1964 Sb., občanský zákoník (OZ)/ Civil Code (1964) (415, 574(2))

Zákon č. 480/2004 Sb., zákon o některých službách informační společnosti / Statute on selected services of information society (4, 5, 6)

Zákon č. 127/2005 Sb., zákon o elektronických komunikacích / Electronic Communications Statute (§ 97(3))

Zákon č. 40/2009 Sb., trestní zákoník (TZ)/ Criminal Code (2009) (15-19, 23-24, 180, 182-183, 230, 231, 232, 248, 253, 367, 368)

Zákon č. 89/2012 Sb., občanský zákoník (NOZ)/ Civil Code (2012) (1725, 1914, 2898, 2900, 2901, 2902, 2903, 2908, 2909, 2910, 2911, 2912, 2913, 2939-2943)

Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti / Cybersecurity Act (Statute no. 181/2014 coll.).

Case law

NS(Rt) 11TDo 919/2004.

32 Odo 1180/2004.

25 Cdo 1369/2006.

25 Cdo 1448/2006.

25 Cdo 2258/2008.

3 Cmo 197/2010-82.

1 Cmo 303/2013-166.

2.7. Others

Art. I:1:103, VI-3:102 Draft Common Frame of Reference

Art. 1383 French Code Civil

French Cour de Cassation 6 October 2006, case 05-13.255

French Cour Constitutionnel, decision no 2009-580, 10 June 2009.

Annex 3. Abbreviations

ACM	Autoriteit Consument en Markt (Netherlands Authority for Consumers and Markets)
ABGB	Allgemeines Bürgerliches Gesetzbuch (Austrian Civil Code)
ALI	American Law Institute
API	Application programming interface
BGB	Bürgerliches Gesetzbuch (German Civil Code)
BrCC	Brazilian Civil Code
BrCDC	Brazilian Code of Consumer Protection
BRIC	Brazil, Russia, India and China
BW	Burgerlijk Wetboek (Dutch Civil Code)
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CMS	Content Management System
DDoS	Distributed Denial-of-Service
DMCA	Digital Millenium Copyright Act
DNSSEC	Domain Name System Security Extensions
DVD	Digital Versatile Disc
EC	European Commission
ECJ	European Court of Justice
ECLI	European Case Law Identifier
ECP	Electronic Commerce Platform
EEC	European Economic Community
EU	European Union
FCC	Federal Communications Commission
FENIT	Federatie van Nederlandse Ondernemingen in de Informatietechnologie (Federation of Dutch Information Technology Industry)
FFIEC	Federal Financial Institutions Examination Council
FTC	Federal Trade Commission
FTP	File Transfer Protocol
HR	Hoge Raad (Dutch Supreme Court)
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IRC	Internet Relay Chat
ISO	International Organization for Standardization
ISP	Internet Service Provider

IT	Information Technology
ITU	International Telecommunication Union
LJN	Landelijk Jurisprudentie Nummer
NCUA	National Credit Union Administration
NJ	Nederlandse Jurisprudentie
NJB	Nederlands Juristenblad
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Cooperation and Development
OpenSSL	Open Secure Socket Layer
OS	Operating System
P2P	Peer-to-peer
PHP	PHP: Hypertext Preprocessor (originally: Personal Home Page)
POP₃	Post Office Protocol 3
PSN	Playstation Network
RAM	Random Access Memory
s.	section
SaaS	Software as a Service
SAP	Systemen, Anwendungen und Produkte SE
SCADA	Supervisory Control and Data Acquisition
SIIA	Software and Information Industry Association
SLA	Service Level Agreement
SQL	Structured Query Language
TCP	Transmission Control Protocol
Tw	Telecommunicatiewet (Dutch Telecommunications Act)
UCC	Uniform Commercial Code
UCITA	Uniform Computer Information Transactions Act
UETA	Uniform Electronic Transactions Act
UNODC	United Nations Office for Drugs and Crime
USAM	United States Attorneys' Manual
U.S.A.	United States of America
USB	Universal Serial Bus
U.S.C.	United States Code
USIIA	United States Internet Industry Association
WBRv	Wetboek van Burgerlijke Rechtsvordering (Dutch Code of Civil Procedure)
WCAM	Wet Collective Actie Massaschade (Dutch Collective Claims Act)
WiFi	Wireless Fidelity
WPNR	Weekblad voor Privaatrecht, Notariaat en Registratie
WvSr	Wetboek van Strafrecht (Dutch Criminal Code)

Annex 4. Glossary

Blacklist(ing)	A technique whereby non-profit and commercial organisations may contribute to combating botnets, spam and the distribution of malware. It consists of an organisation keeping a list of ‘suspect’ IP addresses. Subscribers to the particular blacklist can then refuse to allow traffic to and from the blacklisted addresses. (4.4.5)
Botnet	A group of malware infected computers (also called “zombies” or bots) that can be used remotely to carry out attacks against other computer systems. (4.5.3)
Botnet clients	The computers (or the botnet malware on those computers) that have become part of a botnet.
Botnet herder	The individual who commands and controls a botnet. (4.2)
Bounty programs	A practice whereby a reward (bounty) is offered for first-time reporting of bugs, in particular bugs that are vulnerabilities. (4.4.3)
Buffer overflow	A software bug whereby the amount of memory reserved for a software routine is exceeded, with the result that data is being written in other parts of the memory, which can lead to execution of code contained in that part of the data. (4.4.3)
Bug	Software error. (4.4.3)
DDoS attacks	Concentrated attacks on a website server or groups of servers that are designed to render the website unavailable (which leads to a Denial of Service). (4.6.3)
Deep Packet Inspection	Examining the content of Internet communication (which is transmitted in discrete ‘packets’ of bytes; ISPs normally only examine the headers of the packet and not the content). (4.2)
Embedded software	Software that is part of hardware and is not directly accessible to the user, i.e. is embedded within the equipment. An example is the software of a washing machine.
Exploit	Bug that can be exploited by criminals (4.4.2)
Firewall	Software tool that limits Internet communication by only allowing certain kinds of channels and/or programs to communicate (4.5.4)
Freeware	Software made available for free (4.3)
Hacking	Intentionally trying to obtain access to a computer without the computer owner’s knowledge.
Hosting	Store content and and make the content available through the Internet (4.3)

Internet Service Providers	Organisations that provide specific services central to the operation of the Internet. (4.3)
Jailbreaking	Removing security features of a system to allow installation of content that otherwise would be disallowed by the system, such as software not accepted by the app store. This may involve completely removing the original operating system from the device. (4.4.2)
Keyloggers	Malware that logs all keyboard input and transmits the logs to another computer (4.5.2)
Malware	“A piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners” (OECD 2008: 10). (4.5.2)
Mere Conduit	Transmission only, referring to Internet service providers who only transmit data without any interference.
Notice and takedown	The practice that hosting ISPs if properly notified of arguably illegal content upon receipt of the notice subsequently take down the content.
Open source software	Software that is provided for free, with the source code being made publicly available and with the condition that others may freely modify the code provided that any modifications made are also made available for free, publicly, on the same conditions. (4.4.3)
Outsourcing	Contracting with an external IT service provider to perform IT services that previously were provided by employees of the business itself.
Patches	Updates to software that fix bugs in the software.
Pop-up blockers	An Internet browser facility or extension that disallows websites from being able to open new Internet browser windows (that ‘pop up’ in front of the previous window).
Ransomware	Malware that attempts to extort money from a victim by encrypting files and demanding payment for their restoration. (4.6.2)
Shrink-wrap license	A license that aims at becoming accepted through the act of the user opening the shrink wrap which encloses the physical software package (containing a diskette, CD or DVD).
Software as a Service	Software made available as a service, i.e. the software is installed only on computers of the service provider. (4.3)

Spam	Unsolicited e-mail.
Spyware	Malware that spies on the user (4.5.2)
Wizards	Part of a program that guides the user through the configuration process for the program. (4.3)
Zombies	Botnet clients (4.5.3)

Annex 5. Advisory committee

Mrs. Drs. E.C. van den Heuvel (Cyber Security Council), chair

Mrs. Leonie M. Ebbekink, LLM (Legal & Compliance Manager Benelux at ACE Group)

mr J.M. van der Hoek (projectleider wet- en regelgeving, DGETM, directie Telecommarkt, Ministerie van Economische Zaken)

Drs. Liesbeth Holterman (beleidsadviseur Nederland ICT)

Mr. drs. D.P.L. Ter Laak (Beleidsmedewerker Parket-Generaal Openbaar Ministerie)

MA Bart Pegge (beleidsadviseur Nederland ICT)

Drs. J.P. Raeven (Beleidsadviseur, Directie Rechtshandhaving en Criminaliteitsbestrijding, Ministerie van Veiligheid en Justitie)

Drs. B. Sluiter (Senior beleidsmedewerker, Nationaal Coördinator Terrorismebestrijding en Veiligheid/Directie Cyber Security)

Drs. Eelco Stofbergen (Hoofd Expertise & Advies, Nationaal Cyber Security Centrum)

Annex 6. External academic review

United States of America:

prof. S.W. Brenner (Professor & Samuel A. McCray Chair in Law, University of Dayton School of Law)

Brazil:

dr. Mario Viola (Instituto de Tecnologia e Sociedade do Rio de Janeiro)

Czech Republic:

doc. JUDr. Radim Polčák Ph.D., Mgr. Václav Stupka, Mgr. Jakub Harašta (Institute of Law and Technology, Masaryk University, Brno, Czech Republic)